Trusted Platform Module and Privacy:

Promises and Limitations

Ron Kim
Department of Computer Science
The University of Auckland
skim093@ec.auckland.ac.nz

Abstract

Trusted Computing is an initiative backed by the Trusted Computing Group (TCG) which aims to provide an enhanced level of security through a combination of software and a specialized hardware device, Trusted Platform Module (TPM). TPM is a microcontroller that provides protected storage of sensitive data and a way for remote attestation to third parties. With its promoters including big name players such as Microsoft, Intel Corporation, AMD and IBM, the technology is making sure footed steps towards the mass market. The paper examines the TPM and its potential merits and limitations in upholding users' privacy.

1. Introduction

With the recent release of a specification for Trusted Computing (TC) by the Trusted Computing Group (TCG), awareness, along with controversies, has surged. The TCG is an organization that designs and develops specifications for trusted computing and security technologies [3]. While there exist several initiatives that fall under the broad umbrella of "Trusted Computing", the paper focuses on TC as specified by the TCG. TC is a massive and ambitious initiative, backed by numerous giant corporations such as Microsoft, Intel Corporation, AMD and IBM, and is surely on its way to the mass market.

Trusted Platform Module (TPM) is a small microcontroller device that can be integrated in most computing devices such as PC, laptop and mobile phones. It plays a vital role in TC of acting as a "root of trust" for a platform in a sense that it is intrinsically trustworthy, being tamper-evident. It comes with numerous features that can affect users' privacy: integrity measurement, storage and report, protected storage of sensitive data and remote attestation.

The paper discusses how the TPM could be used to protect users' privacy and its limitations in doing so. The structure of the paper is as follows. In section 2, the paper introduces the concept of Trusted Computing and related background information. Section 3 provides a number of definitions of terminologies used in the paper. Section 4 briefly describes features of TPM and introduces associated protocols. Section 5 discusses potential benefits and limitations of the TPM in protecting users' privacy. Section 6 concludes the paper with a summary of the paper.

2. Trusted Computing

Trusted Computing (TC) is a generic term that describes a technology which, through a combination of software and hardware enhancements, aims to provide a way to prove that a platform is in a software state that it claims it is in. It is an ambitious initiative that would allow users and third parties to verify a platform is in a state that is known to be secure. TC encompasses several initiatives including Next-Generation Secure Computing Base (NGSCB) by Microsoft, LaGrande by Intel Corporation and Trusted Computing Platforms by the Trusted Computing Group (TCG). In essence, all these initiatives strive to achieve a similar objective. In this paper, TC refers to Trusted Computing Platforms initiative driven by the TCG.

The TCG is an organization, formerly known as the Trusted Computing Platform Alliance (TCPA), which promotes and develops specification for trusted computing and security technologies [3]. With its promoting members including big name players such as Microsoft, Intel Corporation, AMD and IBM to name a few, TC is making sure footed progress towards the mass market, with some products already available.

As with most initiatives of such a scale, TC has been at the center of controversies. There have been numerous accusations, one of the infamous being that by Ross Anderson of Cambridge University [1] accusing TC as being an anticompetitive technology designed to lock-in users and to enforce DRM. While some accusations represent various potential misuses of the technology including privacy issues, many remain as subjective speculations. Thus, an objective analysis of TC is necessary so as to inform the potential users the prospective implications of the technology. The paper focuses on potential implications on its users' privacy, both its promises and limitations.

3. Definition of Terms

In order to examine the implication of TPM on users' privacy, it is first necessary to define what privacy means. RFC2828 defines privacy as "[t]he right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others" [5]. In other words, privacy is preserved if a user of a TPM can determine “what information related to them may be collected and stored by whom and to whom that information may be disclosed” [5].

As with privacy, the term ‘trust’ is used with subtle differences in meaning often causing confusion; hence a definition is required to aid understanding. According to RFC2828, ‘trust’ is “[t]he extent to which someone who relies on a system can have confidence that the system meets its specifications” [5]. In other words, a trusted system behaves in an expected way. An important question that is often raised regarding such a use of the term ‘trust’ is, “Trusted by who, to do what?” [4]. The opinion of the author is that TPM is trusted by the TC system to provide a secure storage and report a correct state of the platform it is in, and any tampering is detected.

4. Trusted Platform Module

At the core of TC technology resides Trusted Platform Module (TPM). It is a microcontroller which can be integrated into a PC, laptop and various computing devices essentially to provide safe storage of sensitive data and key generation for remote attestation. A key feature that enables the above two features is integrity measurement, storage and reporting.

The TPM is given a pair of RSA keys called endorsement keys (EK) at the time of manufacture [3]. EK is a public-private key pair and is unique to a TPM. As will be discussed in the sections below, EK plays a pivotal role in remote attestation.

The TPM is “trusted” in a sense that it assumed that it cannot be tampered with without leaving a trace, i.e. tamper-evident, and that it operates according to its specifications. However, it should be noted that the TPM is not designed to be tamper-resistant as it is rather vulnerable to power analysis, which can extract protected cryptographic keys by analyzing power consumption of CPU [7], and local hardware attacks [8].

4.1 Integrity Measurement, Storage and Reporting

Integrity measurement involves the TPM obtaining “integrity metrics of platform characteristics that affect the integrity (trustworthiness)” [13]. For instance, the platform characteristics could include the machine’s hardware configurations or software it is running. Integrity metrics are measured and validated, and then its hash is stored in shielded locations called Platform Configurations Registers (PCR’s).

It represents a key feature which allows and adds value to protected storage and remote attestation features. Remote attestation and access to sensitive data are allowed only when the stored values in PCR’s and the current integrity metrics match, i.e. when a platform is in a valid, secure state.

4.2 Protected Storage

Sensitive data could include but not limited to cryptographic keys, passwords and digital certificates. The TPM provides a protected storage for such data by encrypting the secret data with a private key that only the TPM has access to. In addition, the TPM can bind the sensitive data to a platform by encrypting the sensitive data along with platform configuration values. Access to the sensitive data is only allowed when the stored and current platform configuration values match. In effect, protected storage feature of the TPM equates to a ‘lock’, as used by Lampson [6], which raises the threshold for a break-in thereby reducing the threat of an attack. Additionally, as mentioned earlier sensitive data can be less vulnerable to software attacks as access to it can be disabled at hardware level and compromise in integrity can be determined by the TPM.

4.3 Remote Attestation

Recall that each TPM is given a unique RSK key pair called endorsement keys (EK_{pu} and EK_{pr}). Remote attestation is a process of attesting to a remote party that a TPM has a valid EK and therefore it is a valid TPM. The remote party can then trust the platform that the TPM resides on and conclude that it is safe to exchange data with it. It represents an improvement over what is possible today, as there exists virtually no way of assuring that a remote communication partner’s platform is in a secure or not.

While remote attestation allows some level of trust to be established between remote communications partners, privacy of users can be threatened due to the fact that the EK pair is unique to the TPM and it can be used to uniquely identify the TPM and thus the user. In other words, the uniqueness of the EK pair may enable remote parties to create a profile of user’s activities without user’s consent.

4.4 Overview of Remote Attestation Protocols

Efforts have been made by the TCG and fellow researchers to develop a protocol that minimizes the threat to user's privacy. The TCG specified two protocols for remote attestation. The first protocol, which relies on use of a trusted third party termed Privacy CA. The procedure is as follows (after 5):

1) TPM generates a second key pair: RSA Attestation Identification Key (AIK) pair
2) TPM sends its $\mathrm{AIK}_{\mathrm{pu}}$ to Privacy CA along with extra certificates
3) Privacy CA validates the request and issues a certificate with respect to AIK
4) The certificate on AIK is used to prove to a un-trusted remote party that it is indeed a valid TPM

As the TPM is allowed to obtain many AIK's, different AIK's could be used for transactions with different un-trusted remote parties thereby achieving a level of anonymity [3]. However in this protocol, Privacy CA has access to $\mathrm{AIK}_{\mathrm{pu}}$ and therefore is able to uniquely identify a TPM. If Privacy CA colludes with an adversary, all transactions of the TPM become linkable to its user and therefore profiling becomes possible. Moreover the protocol is considered to be infeasible by many including J. Camenisch [5] and B. Arbaugh [2].

Therefore a second protocol termed *Direct Anonymous Attestation* (DAA) based on group signatures was developed and incorporated in TPM v1.2 specification [5]. To prove its validity to a remote party, the TPM generates and sends a set of DAA-credentials (Nv) which is calculated using its secret key and ζ, which is basically a challenge value from the remote party. It is then possible for the remote party to determine if the TPM is valid by checking that Nv belongs to a group of possible values that are generated by valid TPM's [3].

The protocol is deemed to be more feasible as the requirement for a Privacy CA is removed [5] and disclosure of AIK_{pu} is no longer necessary [12]. However as Camenisch rightly points out, the privacy issue discussed earlier still exists, just in a different form. For the remote party to detect invalid TPM's, ζ needs to stay (relatively) constant. In such a case Camenisch argues it is possible that a remote party can link transactions of a specific TPM and profile them for its use without user's knowledge, this time without the need to collude with Privacy CA [5].

Consequently, a new remote attestation protocol was proposed by Camenisch with an aim to obtain the same level of privacy as the first protocol while remaining as feasible as the second protocol [5]. Camenisch, recognizing that privacy issue arose in the detection mechanism for an invalid TPM; he attempted to avoid the privacy issue by separating the detection mechanism from the servicing of the request. While the proposed protocol may provide the claimed level of privacy, as of yet, it is not included in the TPM specification.

5. Discussions

5.1 Promises

As presented in section 4, the TPM has features that allow a better protection of user's privacy. Sensitive data is stored in hardware, meaning that software-based attacks to retrieve personal information can be subverted if the TPM can detect a compromise in platform integrity and virtually shutdown access to the data stored in hardware. Even when the sensitive data is successfully retrieved by a perpetrator, the data can be inaccessible due to the fact that integrity metrics hashed along with the data will not match on a different platform. In short, the feature makes it hard for an unauthorized party to gain access to confidential information of user, or in short, it helps protects users' privacy.

While the author does not observe any benefits the remote attestation may bring to enhance privacy protection for users, the TPM specification is indeed work in progress. Considering the TCG and researchers recognize the importance of users' privacy as shown in [3], [5] and [12], the author is hopeful there is a chance that the limitations the paper will cite in the coming section will be worked on.

5.2 Limitations

As Camenisch acknowledges in [5], with the Privacy CA protocol personal information, such as a profile of user activities, can be leaked to a third party without users' knowledge if a third party and the Privacy CA collude. As Arbaugh puts it, "[the TCG] proponents may argue, but cannot guarantee that [colluding] will never happen" [2].

While the second protocol is an improvement over the first, it needs to sacrifice user's privacy in order to detect invalid TPM's attestations. The third protocol does claim that even collusion will not result in a leak; however, it is not even clear whether or not the proposed protocol will be included in any future TCG specification.

It should also be noted that the TPM cannot protect against many of attacks that threaten privacy of users. For instance, Ross Anderson protests "Most viruses nowadays exploit the scripting languages in products like [Microsoft] Office" [14]. In such a case, the application may be trusted by TC system however user's activities or data could actually be compromised covertly. Also the TPM does not reduce the threat from the likes of spywares that could monitor and profile user's activities, such as browsing habits, and send them to a remote party. Additionally, as mentioned in section 4 it is vulnerable to power analysis which can break tamper-evident property of the TPM by being able to extract information from protected storage without being detected.

Lastly, while the TCG Best Practices Committee does emphasize the importance of privacy of users of TPM-based systems, it provides little to no way of actually enforcing its guideline to protect users' privacy. Without the means to enforce the guideline, the privacy of users may ultimately end up in the hands of implementers of the TPM specification.

6. Conclusion

Trusted computing, whether you like it or not, is making its progress towards the mass market backed by giant corporations. At the heart of the technology resides the TPM. The paper presented a brief overview of the TPM and its functionalities and discussed the ways it can aid protecting users' privacy and its limitations in doing so.

The TPM was identified to aid protecting users' privacy by providing protected storage that adds an extra layer of hardware protection over sensitive data. Also the TPM allows binding of sensitive data to a platform such that even when an adversary succeeds in stealing the data, it may be unable to extract information. The TPM is claimed to be tamper-evident, meaning that attacks on it do not go unnoticed. All in all, the effect of these features aid in enhancing users' privacy.

Also, the paper identified several limitations of the TPM and its remote attestation protocols in protecting to users' privacy. While remote attestation that is possible with the TPM can be beneficial to security, the paper elicited potential threats to user's privacy resulting from the three remote attestation protocols. Other limitations of the TPM included vulnerabilities from various threats such as spywares, power analysis and exploiting of trusted software.

While the TCG Best Practices Committee does provide a guideline with emphasis on protection of users' privacy, the paper argued that there lacks a way to enforce the guideline and thus users' privacy may not be protected as hoped for.

References

[1] Anderson, R. (2003). *"'Trusted Computing' Frequently Asked Questions"*, available at http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html

[2] Arbaugh, B. (2002). *"Improving the TCPA Specification"*, Computer, Volume 35, Issue 8, August 2002 Page(s) 77-79 available at http://ieeexplore.ieee.org.ezproxy.auckland.ac.nz/iel5/2/22017/01023792.pdf?tp=&arnumber=1023792&isnumber=22017

[3] Bajikar, S. (2002). *"Trusted Platform Module (TPM) based Security on Notebook PCs - White paper"*, Mobile Platforms Group, Intel Corporation, available at http://developer.intel.com/design/mobile/platform/downloads/Trusted_Platform_Module_White_Paper.pdf

[4] Blakely, B. & Kienzle, D. M. (1997). *"Some Weaknesses of the TCB model"*, Security & Privacy, Proceedings.,1997 IEEE Symposium on 4-7 May 1997 Page(s) 3-5, available at http://ieeexplore.ieee.org.ezproxy.auckland.ac.nz/iel3/4693/13107/00601305.pdf?tp=&arnumber=601305&isnumber=13107

[5] Camenisch, J. (2004). *"Better Privacy for Trusted Computing Platforms"*, to appear in ESORICS 2004. Preprint provided in email by J. Camenisch, July 2004.

[6] Lampson, B. W. (2004). *"Computer Security in the Real World"*, Computer, Volume 37, Issue 6, June 2004 Page(s) 37-46

[7] Reid, J., Nieto, J. M. G., Dawson, E. (2003). *"Privacy and Trusted Computing"*, Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop on 1-5 Sept. 2003 Page(s) 383-388, available at http://ieeexplore.ieee.org.ezproxy.auckland.ac.nz/iel5/8719/27592/01232052.pdf?tp=&arnumber=1232052&isnumber=27592

[8] Safford, D. (2002). *"Clarifying Misinformation on TCPA"*, IBM Research, available at file:///home/safford/tcpa/tcpa_rebuttal.html

[9] Shirley, R. (2000). *"Internet Security Glossary"*, available at http://www.faqs.org/rfcs/rfc2828.html

[10] TCG Best Practices Committee. (2005). *"Design, Implementations and Usage Principles for TPM-Based Platforms Version 1.0"*, available at https://www.trustedcomputinggroup.org/downloads/bestpractices/Best_Practices_Principles_Document_v1.0.pdf

[11] Trusted Computing Group. (2005). *"TCG Backgrounder"*, available at https://www.trustedcomputinggroup.org/downloads/background_docs/TCGBackgrounder_revised_012605.pdf

[12] Trusted Computing Group, *"TPM v1.2 Specification Changes"*, available at https://www.trustedcomputinggroup.org/groups/tpm/TPM_1_2_Changes_final.pdf

[13] Trusted Computing Group website. http://www.trustedcomputinggroup.com

[14] Vaughan-Nichols, S. J. (2003). *"How Trustworthy Is Trusted Computing?*", Computer, Volume 36, Issue 3, March 2003 Page(s) 18-20, available at http://ieeexplore.ieee.org.ezproxy.auckland.ac.nz/iel5/2/26595/01185209.pdf?tp=&arnumber=1185209&isnumber=26595