Trusted Computing: Challenges & Solutions

Nor Fatimah Bt Awang

Department of Computer Science
National Defence University of Malaysia, Sungai Besi Camp, 57000, Kuala Lumpur
Tel : 03-90514427, Fax : 03-905134623
E-mail : norfatimah@upnm..edu.my

ABSTRACT

Most citizens of the world today are fighting for – either by battling viruses, spam, phishing or other malware, or by fending off schemes to compromise privacy and extract confidential information. With these worries in mind, the Trusted Computing Group (TCG) was established to develop specifications for trusted computing building blocks and software interfaces that could address the problems and aims to enhance security by using the transitive properties of trust. Unfortunately Trusted Computing is a young technology and struggling with some drawbacks. There are major issues related to technical as well commercial that need to be addressed seriously and carefully. From user's perspective, TC was introduced from desire to prevent users from freely sharing and using potentially technology and seems will introduce more benefits to vendors and large corporations. The main legal concerns are copyright, anti-trust law, data privacy law and digital rights management, the impact on which are not yet clear. This paper will discuss the challenges that currently faced with Trusted Computing in all aspects from different perspective and at the same time provide several solutions to overcome the challenges.

Keywords
Trusted Computing, Security, Network

1.0 INTRODUCTION

There are many promising approaches to improve security in computing environment in all possible angles and aspects eg. redesigning operating systems, changing programming methodologies, or altering the PC's hardware itself. This broad term as well as scope drives a mix of initiatives by individual processor manufacturers, software makers, service providers, networking and Original Equipment Manufacturers (OEM) to respond to the well-known security challenges. Microsoft has started with a software-based project referred as the Microsoft Next-Generation Secure Computing Base, or NGSCB which specifies software changes that take advantage of the security benefits made available by a planned new PC hardware design (Schoen, 2003). On the other hand, Intel and AMD are in midst of developing a processor-based solution namely as Intel's LaGrande Technology (LT) and AMD's Secure Execution Mode (SEM) respectively in order to provide hardware support needed for all the major feature groups in NGSCB.

Therefore a single body or organisation is crucially needed to streamline end-to-end trusted platform requirements and to further drive in developing standard guidelines and specifications. As a result in 8th April 2003, a not-for-profit industry-standards organization namely as Trusted Computing Group (TCG) was formed to develop, define, and promote open, vendor-neutral industry specifications for trusted computing (Intel Whitepaper, 2003).

2.0 OVERVIEW OF TRUSTED COMPUTING

The demand that gave birth to the trusted computing system normally originated from military or security related agencies. They are the users or groups that are very cautious about every single aspect of security threats to their operations and organizations. Therefore most of trusted computing system has been developed according to military security models and requirements. A secure military personal computers built from common off-the-shelf components has been a long dream of the military and security agencies world-wide as it's would save large amounts of money. Common requirements of such a system are as follows (Challener & Yoder, 2008) :

- Any data on the system must be wiped out both before and after it is used
- The system must be able to securely identify itself
- The user must be able to securely identify himself
- Information passed to the system must not be visible during the transfer
- Confidential information on the system must not be available to other processes running on the system

All of these objectives could be accomplished as follows. A system is designed that has no hard disk, but lots of RAM. This is becoming more doable now that 64-bit architecture chips are shipping, but even 2 gigabytes of RAM is sufficient for most purposes especially the fact that RAM is easier to erase than a hard disk. The machine boots to the network over an IPSec card and a server at the other end loads a secure

operating system into the RAM. These requirements have motivate most of sectors related to trusted computing system to innovate or create an integrated platform that cover the criteria. It may now be possible to build such a system using a Trusted Platform Module (TPM) module at its core.

The basis of Trusted Computing, as defined by TCG, is a collection of one or more security devices that can be embedded within a Trusted Computing Platform. The first device defined by TCG is the TPM, which is encapsulated within a Trusted Computing Platform by affixing a single chip to the motherboard or embedding the functionality within another silicon component. The TPM is typically a microcontroller that stores passwords, digital keys, and certificates to provide unique identification. Either a standalone integrated circuit (IC) or embedded in another IC such as an Ethernet controller, the TPM uses standard software interfaces to work with other security methods to deploy secure applications.

The other critical supporting component in completing trusted computing model is TCG Software Stack (TSS). TSS is a module that similar to Microsoft Next-Generation Secure Computing Base module, or NGSCB. The TSS is comprised of modules and components that provide the supporting functionality to the TPM. Based on the TCG specification, certain functions and services are outside of the scope of the TPM hardware. These functions and services are delivered using the host CPU and system memory. The TSS provides the necessary software architecture to support the offloading of security functions from the TPM to the main CPU and memory resources of the system. TSS communications with the TPM can occur either locally or remotely. The TSS provides a standard set of application programming interfaces (APIs) so that application vendors can use the TPM.

2.1 Trusted Platform Module (TPM)

The Trusted Platform Module (TPM) is a hardware chip based installed on PC, PDA and mobile phones motherboards to deliver enhance platform security above and beyond the capabilities of today's software and provides hardware-based protection hardware component that securely stores digital keys, certificates and passwords. Figure 1 shows the Trusted Platform Module (TPM) will be a mandatory component to be installed in all devices such as PCs, PDAs and mobile phones to achieve trusted computing platform objective (TCG Group, 2007).

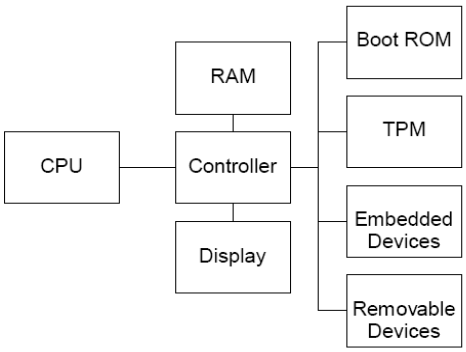

Figure 1: Component installed in devices containing a TCG Trusted Platform Module (TCG Group, 2007)

TPMs protect encryption keys and digital signature keys to maintain data confidentiality. TPM chips are designed to protect key operations and other security tasks that would otherwise be performed on unprotected interfaces in unprotected communications. TPMs are specifically designed to protect platform and user authentication information and unencrypted keys from software-based attacks. Figure 2 shows eleven components embedded into a single TPM platform. The components are Input/Output(I/O), Non-Volatile Storage, Platform Configuration Registers(PCR), Attestation Identity Key(AIK), Program Code, Random Number Generator(RNG), SHA-1 Engine, Key Generation, RSA Engine, Opt-In and Execution Engine (TCG Group, 2007).

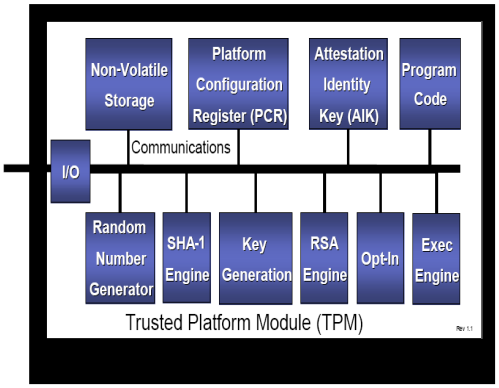

Figure 2: TPM Component Architecture (TCG Group 2007)

2.2 TCG Software Stack (TSS)

Access and control of the TPM operations occurs through the TCG Software Stack (TSS) interface. TSS refers to the supporting software of TPM which supports the access of applications to the TPM[6]. The TSS provides a standard set of application programming interfaces (APIs) so that

application developers can use the TPM, such as Microsoft® CryptoAPI, the Intel® Common Data Security Architecture, and the RSA Security Public-Key Cryptography Standard #11. In this way, the TSS helps enable TPM support for applications using these APIs. Application developers can use the TSS to create interoperable client applications designed to improve tamper-resistant computing by taking advantage of TPM capabilities such as key backup, key migration, platform authentication, and attestation (Molsberry & Berger, 2006).

The TSS is composed of three logical layers: the TCG device driver library (TDDL), the TCG core service (TCS), and the TCG service provider (TSP), each layer has its own standardized definition of interfaces (Challener & Yoder, 2008). The TSP works as the trusted agent of local and remote applications, while the TCS as a trusted server. The TDDL is a library that provides an API to interface with the

TPM device driver.

3.0 POSSIBLE FEATURES IN TRUSTED COMPUTING PLATFORM

The Trusted Computing (TC) offers several features over proprietary hardware security solutions, and inherently, hardware security is stronger than software-only approaches. Existing research shows that the TC can be used to establish trust in the software executing on a computer.

3.1 Storage Protection

This threat arises from the fact that mobile devices or notebook computers are more susceptible to be stolen than their desktop counterparts. Once stolen, notebooks can be subject to a variety of hardware as well as software attacks. It is often found that the stolen data is more valuable than just the cost of the notebook hardware (Bajikar, 2002).

TCG has introduced a Trusted Computing Platform (TCP) that serve a feature of trusted drive that encrypts all data directly on the drive and the encryption speed matches the throughput of the drive interface so the process is essentially unobservable to the user in normal operation. If a trusted drive is stolen, repurposed, or taken out of service, it remains protected. Simple user and security ID keys make end of life and repurposing instantaneous and secure. In the enterprise, a trusted storage system allows authorized access to critical data while preventing unauthorized access or modification of that data.

In addition to an unobservable cryptographic processing of secrets and use of custom logic to provide fast, secure operation for the cryptographic functions, protecting data on a hard drive requires tight access control for secret information. Once again, the TCP provides the key with its hardware-based key generating capability.

3.2 Secure Online Transaction

Notebooks often operate outside of corporate firewalls. Also, they use various means of communication to access the corporate network or the Internet. There are a number of ways in which a determined hacker can attack the communication channel used by the notebook to steal the data being transceived (Bajikar, 2002).

To protect customer and employee data from Internet-based attacks, Personal information Manager (PIM) software, secured by the hardware based chip in TCP, isolates contact information, passwords, bank access codes, and credit card numbers. With multi-factor authentication, some employees reach their programs with a single factor while others require at least dual-factor authentication for network access, providing the appropriate level of security for each department.

Instead of using third-party vendors to encrypt content before backing it up, these transactions are now performed locally in house. With encryption keys residing locally in the TCP, copies are automatically passed to the Key Transfer Manager Server providing both protected and recoverable information.

3.3 Data and network protector from virus and malware

In today's security environment, a worm, virus or other malware on a PC that connects to the network can easily spread across it. Relying on anti-virus and personal firewall software for portable computers is not acceptable for a secure corporate network. An authorized user can gain access to the network from an external site to simply check email. If the user's computer has a virus or rootkit, a software tool that conceals running processes, these unwanted software items can spread to the network. By taking advantage of the TCP, deceptive or lying endpoints can be detected. Using the hardware-based security of the TCP for integrity measurement and remote attestation, the limitations of software-based protection can be overcome. With the TCP, the specification establishes a level of trust in the state of an endpoint and also ensures the presence, status, and software version of mandated applications.

3.4 Digital rights management

Trusted Computing would allow companies to create a digital rights management system which would be very hard to circumvent, though not impossible. An example is downloading a music file. Remote attestation could be used so that the music file would refuse to play except on a

specific music player that enforces the record company's rules. Sealed storage would prevent the user from opening the file with another player or another computer. The music would be played in curtained memory, which would prevent the user from making an unrestricted copy of the file while it is playing, and secure I/O would prevent capturing what is being sent to the sound system. Circumventing such a system would require either manipulation of the computer's hardware, capturing the analogue (and possibly degraded) signal using a recording device or a microphone, or breaking the encryption algorithm (TCG Group, 2009).

4.0 CHALLENGES OF TRUSTED COMPUTING

It is clear that trusted computing hardware provides security benefits when nicely blended with right software that is prepared to take advantage of it. But trusted computing has been received skeptically and remains controversial. Some of the controversy is based on misconceptions, but much of it is relevance. There are too many troubling aspects of TC to ignore, here's more about risks involved in TC.

Any hardware component, including the TC hardware itself, has the potential to fail, or be upgraded and replaced. A user might rightly conclude that the mere possibility of being irrevocably cut-off from access to his or her own information, or to years' worth of expensive work-products, with no opportunity for recovery of that information, is unacceptable (TCG Group, 2009). The concept of basing ownership or usage restrictions upon the verifiable identity of a particular piece of computing hardware may be perceived by the user as problematic if the equipment in question malfunctions.

The TCG only released a specification, but no conformance tests are forced onto the vendors. Up to now, there is no feasible test methods to judge whether they are compliant to TCG specifications or not. Therefore it may be difficult for an end user to tell whether his trusted platform is compliant to the whole specification or only to a subset of it as there isn’t any a prototype with full funtion can test TPM. Non-corformance and bugs of TPM can lead to serious security problems.

Trusted Computing requests that all software and hardware vendors will follow the technical specifications released by the Trusted Computing Group in order to allow interoperability between different trusted software stacks. However, even now there are interoperability problems between the TrouSerS trusted software stack (released as open source software by IBM) and Hewlett-Packard’s stack (TCG Group, 2009)(Zhang, Luo, Yan, Xu, He & Zhan, 2008). Another problem is the fact that the technical specifications are still changing, so it is unclear which is the standard implementation of the trusted stack.

An additional issue is that measurements are computed only when the components are loaded: without proper software architecture for monitoring the platform resources at run-time, nothing can be said about the dynamic behaviour of the components. For example, if a component is altered by a virus at run-time (i.e. after it has been loaded and measured), this fact is not detected (Lioy, Ramunno & Vernizzi, 2007).

The technical idea underlying trusted computing is that the computer includes a digital encryption and signature device, and the keys are kept secret by manufacturers. Proprietary programs will use the TPM to control which other programs can be run, which documents or data can be accessed, and what programs can be pass them to. These programs will continually download new authorization rules through the Internet, and impose those rules automatically, refuses to obtain the new rules periodically from the Internet might causes some capabilities will automatically cease to function (Stallman, 2004).

Trusted computing puts the existence of free operating systems and free applications at risk, as TPM will block this kind of software. Some versions of trusted computing would require the operating system to be specifically authorized by a particular company. Free operating systems could not be installed. Some versions of trusted computing would require every program to be specifically authorized by the operating system developer. To run free applications on such a system could be a crime (Stallman, 2004).

A user who wanted to switch to a competing program might find that it would be impossible for that new program to read old data, as the information would be "locked in" to the old program. It could also make it impossible for the user to read or modify their data except as specifically permitted by the software. Remote attestation could cause other problems. Currently web sites can be visited using a number of web browsers, though certain websites may be formatted such that some browsers cannot decipher their code. Some browsers have found a way to get around that problem by emulating other browsers. With remote attestation a website could check the internet browser being used and refuse to display on any browser other than the specified one (like Internet Explorer), so even emulating the browser would not work.

One of the early motivations behind trusted computing was a desire by media, entertainment and software corporations for stricter DRM (Digital Rights Management) technology to prevent users from freely sharing and using potentially copyrighted or private files without explicit permission. On the other words, the downloaded videos and music can be played only on one specified computer. These are examples of a more general problem of "lock-in", often practiced as a deliberate business strategy in the software industry, to the detriment of business and home computer users alike.

5.0 PROPOSED SOLUTIONS

The TCG technical committee considered few intiatives to improve the weaknesses and risks from the existing TC privacy policies. The TCG privacy model generally follows the privacy guiding principles established by the World Wide Web Consortium (W3C) P3P working group6.

5.1 Notice and Communication

Service providers should provide timely and effective notices oftheir information practices, and user agents should provide effective tools for users to access these notices and make decisions based on them (Cranor, 1998).

5.2 Choice & Control

Users should be given the ability to make meaningful choices about the collection, use, and disclosure of personal information. TCG is committed to enabling owners and users of computing platforms to remain in control of their platform, and to requiring platform owners to opt in to enable TCG features (Cranor, 1998).

5.3 Fairness and Integrity

Users should retain control over their personal information and decide the conditions under which they will share it. Service providers should treat users and their personal information with fairness and integrity. This is essential for protecting privacy and promoting trust (Cranor, 1998).

5.4 Confidentiality

Users' personal information should always be protected with reasonable security safeguards in keeping with the sensitivity of the information (Cranor, 1998).

5.5 Open platform development model

Encourage the open development model that enables any party to develop hardware, software, or system platforms based on TCG specifications, and to preserving consumer freedom of choice (Molsberry & Berger, 2006).

5.0 CONCLUSIONS

The implementation of TC technology seems to have consequences for many people especially related to privacy. TC is primarily seen as a threat to privacy as a political concept, giving multinational companies access to information we would prefer to keep private. Unsurprisingly, the TC has provoked and given rise to number of controversies between its proponents and opponents. This is due to the fact that the aim of TCG will provide more trustworthiness from the point of view of software vendors and the content industry, but will be less trustworthy and freedom from the point of view of their owners.

Fortunately, the TCG as well as independent researchers is working seriously to address the limitations and weakness of the TC. For instance, Open Platform Development Model initiative will improve TC platform openness and flexibility in offering benefits to both vendors and users. TC can be very useful for secure infrastructure commons if its limitations and critical points are carefully taken into account and ultimately will covert all the challenges to opportunities in which will develop a better secured community.

REFERENCES

Bajikar, S. (2002). *Trusted Platform Module (TPM) based Security on Notebook PCs – White Paper*. Retrieved February 2, 2009, from http://www.intel.com/design/mobile/platform/downloads/Trusted_Platform_Module_White_Paper.pdf.

Challener, D., & Yoder, K. (2007). A Practical Guide to Trusted Computing. IBM Press, 77-92.

Cranor, L., F., (1998). P3P Guiding Principles. Retrieved January 5, 2009, from http://www.w3.org/TR/NOTE-P3P10-principles/.

Intel Whitepaper. (2003). *Protecting Your Vital Business Data with Trusted Platform Module*. Retrieved January 28, 2009 from http://www.download.intel.com/design/motherbd/articles/TPMFlyer.pdf.

Lioy, A., Ramunno, G., & Vernizzi, D. (2007). Trusted Computing and Infrastructure Commons. Retrieved February 5, 2009, from http://www.communia-project.eu/communiafiles/ws01p_Communia-TrustedComputingAndCommons.pdf

Molsberry, F., & Berger, B. (2006). *Enhancing IT Security with Trusted Computing Group Standards*. Dell Power Solution, 13-15

Schoen, S. (2003). *Trusted Computing – Promise and Risk*. Retrieved January 28, 2009, from http://www.eff.org/wp/trusted-computing-promise-and-risk.

Stallman, R., M., (2004). Free Software, Free Society : Selected Essays of Richard M. Stallman. Retrieved

January 30, 2009 from http://www.gnu.org/philosophy/fsfs/rms-essays.pdf.

TCG Group. (2007). *Trusted Computing Group. TCG Specification Architecture Overview*. Retrieved January 30 2009 from http://www.trustedcomputinggroup.org/groups/TCG_1_4_Architecture_Overview.pdf.

TCG Group. (2009). *Trusted Computing*. Retrieved January 30, 2009, from http://en.wikipedia.org/wiki/Trusted_Computing.

Zhang, H., Luo, J., Yan, F., Xu, M., He, F., & Zhan, J. (2008) *A Practical Solution to Trusted Computing Platform Testing*, IEEE Computer Society, 79-87.