Trusted Computing – Opportunities & Risks

Nor Fatimah Bt Awang
Department of Computer Science
Faculty of Defense Science and Technology
National Defense University of Malaysia
Kuala Lumpur Malaysia
norfatimah@upnm.edu.my

***Abstract*— Computer security is undeniably important in IT era nowdays. Most computer users 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. However, the implementation of this technology seems to have consequences for many people. At present, there is no standard mechanism for establishing trust in the Trusted Computing (TC) on a particular machine. The TC specification is not rigidly defined when it comes to implementation, leaving many open issues for research and development efforts. There are major issues, especially related to privacy. One big worry is the potential loss of anonymity and the threat of unwanted surveillance and even control. TC also affects areas other than purely technical ones. The capabilities of TC technology have legal as well as economic consequences. 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 TC in concept and study on the opportunities and risks of the system in existing computing system environment particularly related to security matters.**

Keywords-component; Trusted Computing, security, network

I. 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[4]. 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 Next-Generation Secure Computing Base (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[11].

TCG has extended it scope beyond PCs to other devices and system such as storage, mobile devices, servers, infrastructures, and peripherals. A bigger workgroup has been created to define implementation architectures for respective element. The Storage Work Group, for example, plans to build on existing TCG technologies and address standards for security services on dedicated storage systems, such as disk drives, removable media drives, flash storage, and multiple storage device systems. To date, TCG specifications have been developed for desktop and portable computers, mobile devices, storage devices, and the network itself. Of course, these specifications only provide an improved level of trust if they are implemented.

Figure 1. Trusted Computing Group Standard [2]

Digital Object Identifier: 10.4108/ICST.COLLABORATECOM2009.8402
http://dx.doi.org/10.4108/ICST.COLLABORATECOM2009.8402

II. OPPORTUNITY OF TRUSTED COMPUTING

The Trusted Computing (TC) offers several opportunities 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.

A. 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[10].

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.

B. 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 [10].

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.

C. 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.

D. 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[7].

III. TRUSTED COMPUTING CONCEPTS

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[18] :

- 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

Digital Object Identifier: 10.4108/ICST.COLLABORATECOM2009.8402
http://dx.doi.org/10.4108/ICST.COLLABORATECOM2009.8402

- 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 Internet Protocol Security (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.

IV. RISKS 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. Trusted computing (TC) has many implications, including some benefits for large corporations. Here discuss more about risks involved in TC.

A. Attestation

By using Remote Platform Attestation, an unauthorized changes to software can be detected via a network. For the legitimate user, it is a best feature to detect tampering. This attestation technique involve third party to check the software running on the system in order to create certificate to system. This third party can get sensitive information about the user's device and able to influence privacy by linking requests of the customer because of the usage of unique keys like the Endorsement Key. For computer device, attestation technique is performed using hash value. Hash value is created and checked against a database to verify the values as correct. Hash value could be invalid if an unknown program is running on the computing device and thus a service provider can deny services.

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.

B. Hardware Failure

Any hardware component, including the TC hardware itself, has the potential to fail, or to 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[7]. 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. TPM has a unique key and this key identifies a single TPM and also the main key for all further operations. TPM is embedded on the motherboard and all important keys are stored and used inside the TPM. That means for instance a software lisence for a certain computing device could be bound to hardware integrated keys.

C. No Standard Testing Procedure

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.

D. No Interoperability

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

Digital Object Identifier: 10.4108/ICST.COLLABORATECOM2009.8402
http://dx.doi.org/10.4108/ICST.COLLABORATECOM2009.8402

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[7][16]. 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.

E. Cryptographic Issues

TCG uses standard algorithms like RSA and SHA-1. But like SHA-1 will not fulfil near future security requirements and should be substituted by better techniques[15]. Implement cryptographic chips in TPM platform has introduces a lot of security-related improvement and also a lot of memory usage, then it will slow the process.

F. Open Source Software

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[14]. On the other words, the downloaded videos and music can be played only on one specified computer. Digital Right Management technology in Trusted Computing will prevents users from freely sharing and using potentially copyrighted or private files without explicit permission.

G. Malfunction of Software or Application

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[14].

V. RECOMMENDATIONS

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.

A. Notice and Communication

Many software systems need to provide services continuously and uninterruptedly. Meanwhile, these software systems need to keep evolving continuously to fix bugs, add functions, improve algorithms, adapt to new running environments and platforms, or prevent potential problems. This situation makes online evolution an important issue in the field of software maintenance and evolution. On the other hand, one of TPM most important role is to protect data from virus or worm attacks by comparing in and out value as a mechanism to identify threats from outside, for instance the "trusted" boot functions provide the ability to store in Platform Configuration Registers (PCR), hashes of configuration information throughout the boot sequence. Once booted, data (such as symmetric keys for encrypted files) can be "sealed" under a PCR. The sealed data can only be unsealed if the PCR has the same value as at the time of sealing. Thus, if an attempt is made to boot an alternative system, or a virus has back-door the operating system, the PCR value will not match, and the unseal will fail, thus protecting the data.[20]. To overcome the situation, software providers and TPM should provide timely and effective notices of their information practices, software providers and TPM should provide effective tools for users to access these notices and make decisions based on them, eg alarm of pop up message to remind users on mismatch value prior to delete any data automatically.

B. Choice and Control

Currently, the specification from TCG does not allowed the owner of the system or the owner of the computer to load an alternate trusted storage root. It also prevent anyone from running an operating system or running other software of their choice. Users should be given the ability to make meaningful choices about the collection, operating system and applications, and disclosure of personal information[19]. Users should be allowed to completely disabled the TPM or it is easily unplugged as praticed by IBM on LPC bus daugtherboard. Computers or terminals must be workable with or without presence of TPM. TPM should act as an added features and independent in which not inter-dependent with other components or softwares. This feature can avoid sofware developers from abusing the TPM and limit users' choice.

C. Fairness & Integrity

Users should retain control over their personal information and decide the conditions they want it. Service providers should treat users with fairness and integrity. This is essential for protecting privacy and promoting flexibility. Users are permitted to completely disable or modify all endorsement keys in order to give complete privacy and freedom. This basically will offer flexibility to users to reuse or reinstall software to new computers or terminals. This feature is critical for software that bind with TPM in order to operate and open source-source softwares that often changed on source code.

D. Open platform development model

Encourage the open development model that enables any party to develop hardware, software, or system platformsbased on TCG specifications, and to preserving consumer freedom of choice[2]. TPM togther with software developers should make peer-to-peer communication within community easier. Where group of computer (that is safe from outsider

Digital Object Identifier: 10.4108/ICST.COLLABORATECOM2009.8402
http://dx.doi.org/10.4108/ICST.COLLABORATECOM2009.8402

monitoring) are allowed to share-files and information without complex authentication process. This features also will make data-backup activities (on other hardware) become easier.

VI. CONCLUSIONS

One of the frequent issues related to network security is the lack of strong device or machine identities for computer systems connected to the corporate network. For instance, the IP networking industry has purely relied on ethernet MAC address on the NIC hardware of PC client computers to identify the computer as an endpoint within the network the found in. The available Software-only security solutions may not be sufficient to protect networks or information from threats. Even firewalls protecting intranet environments can prove inadequate, especially when software attacks bypass the firewall or originate from internal users.[17] Therefore combination of Hardware & Software based embedded security solutions crucially important element of secure environments.

With Trusted Computing (TC), the computer will consistently behave in specific ways, and those behaviors will be enforced by hardware and software. The primary TCG specifications rely on the Trusted Platform Module (TPM) hardware component, which is in widespread deployment, and the TCG Software Stack (TSS), which developers can use as a foundation for various applications.

Unfortunately Trusted Computing is a young technology and struggling with some drawbacks. For example questions on the issue of privacy, the internet and TC from a new perspective. 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.[5]

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 risks to opportunities in which will develop a better secured community.

REFERENCES

[1] Trusted Computing Group. TCG Specification Architecture Overview, http://www.trustedcomputinggroup.org/groups/TCG_1_4_Architecture_Overview.pdf

[2] Frank Molsberry, Brian Berger, "Enhancing IT Security with Trusted Computing Group Standards," http://www.dell.com/powersolutions

[3] Eimear Gallery, "Who are the TCG and what are the trusted computing concepts?," http://www.trust2008.eu/downloads/Edu_Event_Monday/2_Eimear_Gallery_Who_is_the_TCG_and_what_are_TC_concepts.pdf

[4] Trusted Computing – Promise and Risk, http://www.eff.orgwptrusted-computing-promise-and-risk

[5] Yianna Danidou, "Legal Implications of Trusted Computing," http://www.bileta.ac.uk/Document%20Library/1/Legal%20Implications%20of%20Trusted%20Computing.pdf

[6] Trusted Computing Group. TCG Software Stack (TSS) Specification, http://www.trustedcomputinggroup.org/specs/TSS

[7] Trusted Computing, http://en.wikipedia.org/wiki/Trusted_Computing

[8] Safford, David, "Take Control of TCPA," http://www.linuxjournal.com/article/6633

[9] Siani Person, "Trusted Computing Platform, the next security solution," http://www.hpl.hp.com/techreports/2002/HPL-2002-221.pdf

[10] Sundeep Bajikar, "Trusted Platform Module (TPM) based Security on Notebook PCs – White Paper

[11] Protecting Your Vital Business Data with Trusted Platform Module http://www.intel.com/design/mobile/platform/download/Trusted_Platform_Module_White_Paper.pdf

[12] David Challener, Kent Yoder, "A Practical Guide to Trusted Computing," IBM Press, 2008: 77-92

[13] Burmester, M., and Mulholland, J. (2006) "The advent of trusted computing: implications for digital forensics " *Proceedings of the 2006 ACM symposium on Applied computing*, Dijon, France, 283-287

[14] Free Free Software Free Society: selected essays of Richard M. Stallman, http://shop.fsf.org/product/free-software-free-society/

[15] Ruediger Weis, Stefan Lucks, Andreas Bogk,(2004) TC 1.2 –fair play with the `Frits` chip?

[16] Huanguo Zhang, Jie Luo, Fei Yan, Mingdi Xu, Fan He, Jing Zhan, "A Practical Solution to Trusted Computing Platform Testing".

[17] Thomas Hardjono, " Strengthening Enterprise Application Using Trusted platform Modules,"

[18] A Practical Guide to Trusted Computing, http://my.safaribooksonline.com/9780132398428/ch13lev1sec14

[19] P3P Guiding Principles http://www.w3.org/TR/NOTE-P3P10-principles.

[20] David Safford, (2002), Clarifying Misinformation on TCPA, IBM Research

Digital Object Identifier: 10.4108/ICST.COLLABORATECOM2009.8402
http://dx.doi.org/10.4108/ICST.COLLABORATECOM2009.8402