

**TCPA/TCG and NGSCB: Benefits and Risks for  
Users**

**(HS-IKI-EA-04-608)**

**Peter Ericson (a00peter@student.his.se)**

*School of Humanities and Informatics*

*University of Skövde, Box 408*

*SE-541 28 Skövde, SWEDEN*

Dissertation for a Bachelor of Science degree in Computer Science,  
spring 2004.

Supervisor: Jesper Holgersson

**TCPA/TCG and NGSCB: Benefits and Risks for Users**

Submitted by Peter Ericson to the University of Skövde as a dissertation for the degree of B.Sc., in the School of Humanities and Informatics.

**2004-06-06**

I certify that all material in this dissertation which is not my own work has been identified and that no material is included for which a degree has previously been conferred on me.

Signed: \_\_\_\_\_

## **TCPA/TCG and NGSCB: Benefits and Risks for Users**

**Peter Ericson (a00peter@student.his.se)**

### **Abstract**

Trusted computing has been proposed as a way to enhance computer security and privacy significantly by including them in the design of computing platforms instead of adding them on top of an inherently insecure foundation; however, the project has attracted much criticism. This dissertation looks at trusted computing from the user perspective. Possible beneficial uses of the technology are brought up, and some of the raised criticism is discussed. The criticism is analyzed in an attempt to find out if the criticism is correct on all points, or if some of it is the result of misinformation or misunderstanding. The conclusion is that not all the arguments against trusted computing are correct, and that the possible implications for users are taken into account in the development process. The dissertation ends on a positive note, concluding that trusted computing is possible without the worst fears of the critics coming true.

**Keywords:** TCPA, TCG, NGSCB, Trusted computing

# Table of Contents

<b>1 Introduction.....</b>	<b>1</b>
<b>2 Background .....</b>	<b>2</b>
2.1 Security and Privacy .....	2
2.1.1 Security.....	2
2.1.2 Privacy .....	3
2.1.3 A New Approach to Computer Security and Privacy .....	5
2.1.4 Summary.....	6
2.2 TCPA/TCG .....	6
2.2.1 What Is TCPA/TCG? .....	6
2.2.2 Trust and Trusted Platform.....	7
2.2.3 Important Terms and Entities in TCPA/TCG.....	8
2.2.4 How Does It Work?.....	9
2.2.5 Summary.....	12
2.3 NGSCB .....	12
2.3.1 What Is NGSCB? .....	12
2.3.2 Important NGSCB Terms.....	13
2.3.3 How Does It Work?.....	15
2.3.4 Summary.....	17
<b>3 Problem Description.....</b>	<b>18</b>
3.1 Problem Specification .....	18
3.2 Motivation .....	18
3.3 Purpose .....	19
3.4 Expected Result.....	19
<b>4 Method and Approach .....</b>	<b>20</b>
4.1 Method .....	20
4.2 Approach .....	21
<b>5 Analysis .....</b>	<b>22</b>
5.1 TCPA/TCG and NGSCB Benefits .....	22
5.2 TCPA/TCG and NGSCB Criticism and Replies to It .....	24
5.2.1 Digital Rights Management (DRM).....	24
5.2.2 Privacy .....	26
5.2.3 Anti-Piracy Systems and Remote Censuring .....	28

5.2.4 Open-Source Software and Lock-In Scenarios .....	29
5.2.5 Owner Override: A Proposed Solution That Does Not Work? .....	30
5.3 Summary .....	31
<b>6 Conclusion .....</b>	<b>32</b>
<b>7 Discussion .....</b>	<b>34</b>
<b>References.....</b>	<b>36</b>

# 1 Introduction

Traditionally, security has been seen as something that is added on top of computer hardware and software. This has worked fairly well, but there is one fundamental problem with this approach: as attacks on computers become more sophisticated, it is no longer possible to take for granted that the hardware and software on which current security features are based can be regarded as trusted and safe. If the foundation of these security features cannot be completely trusted, do such features provide sufficient security? The answer is that they do not. Malicious users or code could circumvent security features since the foundation on which they are based is insecure.

The TCPA (Trusted Computing Platform Alliance) and more recently the TCG (Trusted Computing Group) have proposed a solution to this and related problems. The idea is to provide security and privacy at the fundamental level to form a trusted foundation for computing. Security should not be something that is added on top of an insecure basis; rather it should be present at the fundamental level. The TCG was formed in April 2003 and it superseded the TCPA (TCG, 2003a). The term “TCPA” is nevertheless still widely used, and therefore the term “TCPA/TCG” will be used in this dissertation when referring to the work previously done by the TCPA and now by the TCG.

Microsoft has developed its own project for trusted computing: NGSCB (Next-Generation Secure Computing Base), formerly know as Palladium. It is based on the work of the TCPA/TCG, but there are differences between TCPA/TCG and NGSCB.

Much criticism has been raised against trusted computing, and there are important issues of user privacy to consider. This dissertation will bring up benefits of trusted computing for users, and some of the criticism will be analyzed and discussed in the light of the information that is available from the organizations that are developing trusted computing. Related issues will be brought up where appropriate.

A background of TCPA/TCG and NGSCB will be given in Chapter 2, where security and privacy will also be discussed briefly. Chapter 3 contains the description of the problem, which is the starting point for the rest of the dissertation. The next chapter, Chapter 4, will describe how the problem was approached. Chapter 5 is the main part of the dissertation: it is here that the problem will be analyzed and discussed. Chapter 6 provides the conclusion of this dissertation. A more general discussion concerning what has been brought up previously in the text will be given in Chapter 7.

# 2 Background

This chapter is concerned with security and privacy in general, and it gives a description of TCPA/TCG and NGSCB. These descriptions are not exhaustive and do not go deeply into all aspects of the two systems; however, all the relevant features are discussed in as much detail as is necessary for the purpose of this dissertation.

## 2.1 Security and Privacy

This section contains a general discussion of security and privacy in the context of computers: what the terms mean and why they are important. It begins with a description of how security and privacy have been previously addressed, and ends with a new approach that has emerged quite recently and that promises to enhance computer security and the protection of privacy by including them in the basic design of computer systems.

### 2.1.1 Security

Today computers and networks are important to our society and they are becoming increasingly important at the level of the individual as well. The more things depend on computers, the more essential it is that they are protected from threats of various kinds, such as physical damage, unauthorized access, and malicious software (Russell & Gangemi, 1991). In a society whose daily functioning depends on computers, it would be a complete disaster if something happened to them that caused the computers to malfunction. Examples of such events are software bugs, faulty hardware, virus infections, and corrupted data.

In the beginning, when computers were rare, they only needed protection from physical threats, which include theft, unauthorized persons operating them, and natural disasters such as floods and earthquakes. Providing such protection was not very difficult as most people did not have access to the computers or knew how to operate them. The only people who were allowed to use the computers were the operators (Russell and Gangemi, 1991). As technology developed, the conditions changed. When computers moved out of dedicated computer rooms and into our homes, and with the advent of networking, the old way of protecting computers was no longer adequate. New means of protection needed to be developed to keep up with the threats introduced by the change in how computers were used (Russell & Gangemi, 1991).

Ever since computers became widely available and connected to each other in networks, protecting information has been of the utmost importance. Not only is there a need for protection against unauthorized local users, but also from things such as viruses and other malicious software, unauthorized remote users, and disclosure of personal and sensitive data without the owner's consent (Pfleeger, 1997).

## 2 Background

Presently, the definition of computer security has evolved and now includes aspects that were not originally part of the definition. The three aspects of computer security today are, according to Pfleeger (1997), the following:

- Availability: authorized entities should have access to the data.
- Confidentiality: authorized entities are the only ones that are allowed to access the data.
- Integrity: authorized entities can create, change, and delete data.

To guard against viruses and malicious code there is antivirus software that recognizes these threats by using a virus signature file. Pfleeger (1997) writes that signatures are the signs by which a virus can be recognized (how the virus operates). A signature file contains known characteristics of dangerous bits of code that allow antivirus software to identify malicious code and possibly remove it and fix files that might have been infected. It is obvious that the signature file needs to be regularly updated in order for the antivirus software to keep up with the latest threats as new ones are continually developed and discovered. The antivirus software will not be able to protect systems from new viruses if it does not know how to find and then deal with them.

Another threat to computer systems stems from the fact that every Internet-connected computer can potentially fall victim to remote users that try to break into it or use it as a starting point for further attacks. Firewalls are used to prevent unauthorized access to computer systems and information from the external world by limiting incoming connections (Chapman and Zwicky, 1995). In addition to this, firewalls also make sure that only authorized outbound connections can be established. The latter is useful for stopping things such as leakage of information and software that "phones home," e.g., the software contacts the developers and sends for example usage statistics or reports about the computer environment in which it has been installed. As an example, the firewall could be told to let outbound connections be initiated only by the Web browser. If another application, such as spyware, tries to establish an outbound connection to send information back to its developers, the firewall will deny this request. (Chapman & Zwicky, 1995).

### 2.1.2 Privacy

As Cavoukian and Tapscott (1997) point out, privacy is difficult to explain, yet most people know what it is about, and the conclusion that can be drawn is that what different people include in the term "privacy" is subjective. One aspect of the protection of privacy that is important is "*maintaining control over the information that is circulating about you—informational privacy*" (Cavoukian & Tapscott, 1997, p. 12), and another aspect—territorial privacy—is to establish and defend a private sphere that the outside world is not allowed to enter. There is also what Cavoukian and Tapscott (1997) call "privacy of the person," which concerns the human body and such things as medical examinations and the taking and storing of for example skin cells and blood. Other types of privacy also exist, such as workplace privacy.

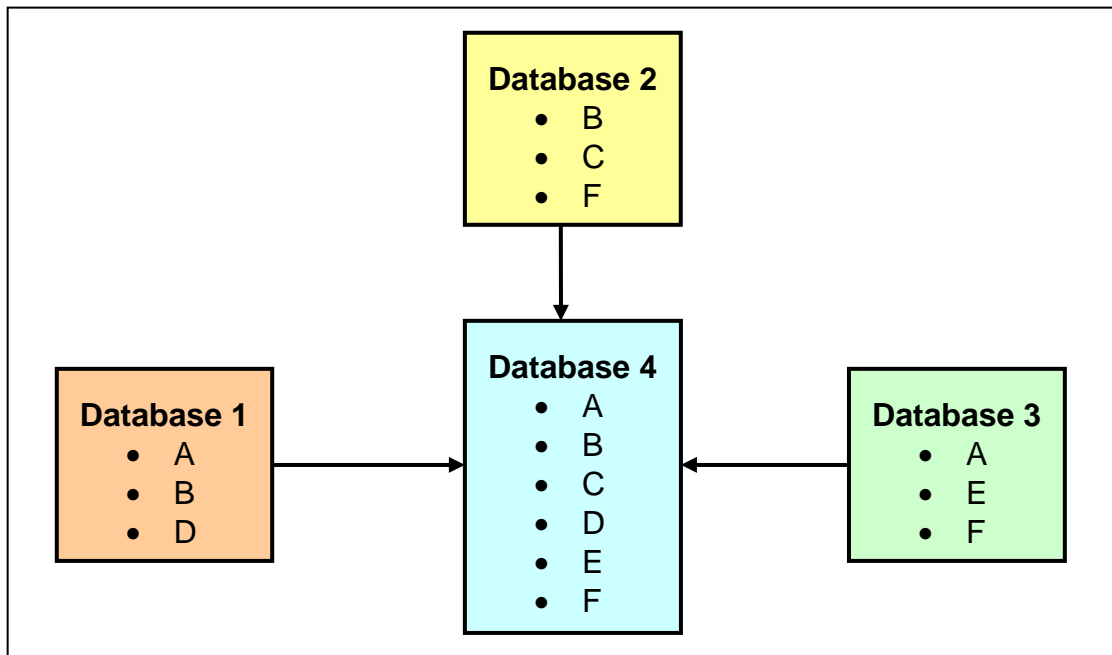
## 2 Background

However, "[d]efinitions of privacy have been as simple as the well-known words of Louis Brandeis of the United States Supreme Court in 1890: 'the right to be let alone.'" (Cavoukian & Tapscott, 1997, p. 11)

In this dissertation, the word "privacy" is taken to mean what Cavoukian & Tapscott (1997) call informational privacy. The person to whom the personal information belongs should be the one who has the ultimate control over when and under what circumstances this information is released to other parties, and for what purposes those parties use the released personal information. Furthermore, even after the information has been released, the person it concerns should have control over the information so that he or she can demand that any errors in it be corrected and that the information be used for requested services only, and not for things such as direct marketing.

Before computers became widely available, privacy was not as big an issue as it is today (Cavoukian & Tapscott, 1997), the reason being that personal information was much harder to obtain due to the fact that it was all stored on paper. Furthermore, with personal information only available on paper at certain locations, it was much more difficult and took a very long time to combine the different records for the purpose of compiling a comprehensive file containing all known personal information of an individual.

Today personal information is stored in digital format and can therefore easily be distributed to other locations—even to the other side of the planet—in no time at all, and digital databases can be quickly merged by powerful computers. This opens up the possibility of cross-referencing and merging different databases, something that makes it possible to build detailed profiles of individuals, and such profiles could then be used for targeted advertisements, among other things. Clearly, this is a potential threat to privacy. The more information that is stored in various databases, the bigger the threat, and if different databases are linked to each other, it will be possible to build one big database containing information about individuals gathered from the linked databases (a simple example of this is shown in Figure 1).



**Figure 1.** It is possible to get a much more comprehensive profile of individuals by merging databases that contain different data about the individuals (databases 1–3) into one database (database 4). This requires that each database participating in the merged database contain at least some identifying data.

### 2.1.3 A New Approach to Computer Security and Privacy

As can be seen from the two previous sections, the necessity of protection has changed drastically from the beginning of the computer era to the present time. Current methods to handle security and privacy problems are based on the addition of software, or in some cases hardware, thus seeing security and privacy as external issues from the viewpoint of the system itself. A new way of fulfilling the requirements of security and privacy is required to keep up with the current technological developments in the area of computing. Time has come to take security and privacy in computing to the next level by introducing a new approach.

This new approach is low-level security and integrity protection, which means that protection mechanisms must be present in the basic hardware as well as in the BIOS (Basic Input/Output System) and in the operating system (TCPA, 2002c). Security and privacy needs to be integrated in the system instead of being added on top of it in an ad hoc manner. Software on its own cannot provide the trustworthiness that is needed to keep up with the technological progress and the possibilities and threats that come with it (TCPA, 2000). There is nothing an operating system—no matter how secure it is—can do to counter the threat of unauthorized software executing before the operating system has loaded and taken control of the system. Therefore, the starting point must be a device that can be trusted and cannot be modified, and this device can then ensure that other devices in the system can be trusted.

## 2 Background

### 2.1.4 Summary

Security and privacy have become very important issues in an increasingly digitalized world. There are many options available that provide security and ensure personal privacy, but they take an external approach in that security and privacy are added on top of the system. A different thinking in which security and privacy are seen as inherently internal has emerged. In this thinking, software alone cannot guarantee security and privacy; an additional part is needed, and this part is provided by hardware. The need for security and privacy to be seen as fundamental parts in a computer system has emerged from the fact that current methods of providing security and privacy have their limits and can potentially become inadequate or even obsolete in a not-too-distant future.

## 2.2 TCPA/TCG

In this section, an overview of TCPA/TCG is given and related terms and concepts are discussed. TCPA/TCG introduces new hardware functions that will verify and measure the state of computer systems. These verifications and measurements are then used to ensure that the systems can be considered trustworthy in communications with other systems.

### 2.2.1 What Is TCPA/TCG?

The TCPA is an alliance that was formed in 1999 by five companies (Compaq, HP, IBM, Intel, and Microsoft) with the purpose of providing a foundation for trusted computing by developing a standard that specifies how trusted computing can be implemented (TCPA, 2002a).

On April 8, 2003, the creation of the TCG was announced (TCG, 2003a). The group was founded by AMD, HP, IBM, Intel, and Microsoft. The TCPA members were invited to join the TCG (there was no automatic transfer of members), and the work of the TCPA was taken over by the TCG to be further developed (TCG, 2003a).

The list below contains the aims of the TCPA/TCG and trusted computing (TCPA, 2002a):

- Create a standard for computer and information security that is independent of the platform on which it is implemented.
- Protect sensitive data by providing *protected storage*.
- Make it possible for computing devices to authenticate and identify themselves in a way that cannot be abused or falsified (*remote attestation*).
- Put the control of privacy and integrity information in the hands of the users.

## 2 Background

The TCPA/TCG should provide *"a ubiquitous and standardized means to address trustworthiness of computing platforms"* (TCPA, 2002b, p. 4). In another document, the mission is stated like this: *"[t]o maintain the privacy of the platform owner while providing a ubiquitous interoperable mechanism to validate the identity and integrity of a computing platform"* (TCPA, 2002c, p. 2).

TCPA/TCG is not limited to a certain platform, and can therefore be implemented on all kinds of computing devices, such as PCs, cell phones, and personal digital assistants (PDAs), although that requires a specification that is specifically suited for each kind and also in accordance with the general platform-independent specification (TCPA, 2002a).

### 2.2.2 Trust and Trusted Platform

Trust is defined in the following way by the TCPA (2001, p. 4): *"an entity can be trusted if it always behaves in the expected manner for the intended purpose."* This is the behavioral definition. This definition of trust is, however, not the only one. Pearson (2002) discusses a social definition of trust:

*"The social component of trust relates to what it is to be trustable (capable of behaving properly); that is, trustworthy in a social sense, when people agree that the trusted item is bona fide and will do the right things"* (p. 4).

The social aspect is *"an expression of confidence in behavioral trust"* (Pearson, 2002, p. 4). Social trust is present in the context of TCPA/TCG: in the case of certificates that state that the trusted computing components in a certain platform are in accordance with TCPA/TCG, for example (Pearson, 2002). Here it is not about how the components actually behave, but what is important is that the designers of the platform assure you that it complies with TCPA/TCG. Pfleeger (1997, p. 270) writes that trust *"is a quality of the receiver, not of the giver,"* which is exactly the case with TCPA/TCG.

If a platform can be trusted by both local and remote entities, then it is referred to as a trusted platform (TCPA, 2001). The idea is that a platform should be able to make reliable measures and correctly report how it is operating. This information can then be matched against the results that would be expected from a platform that operates correctly; for example, the measured integrity metrics are compared to a list of integrity metrics characteristic of a computer running an acceptable configuration as defined by the remote party. There is a need for authorities to provide the results that the matching is performed on, and these authorities must be trusted by both the platform and the entity on the other end (TCPA, 2001). The user operating the local platform and/or a remote party can then make judgments based on this information, depending on for what the platform will be used. The requirements will of course vary since different remote parties will have different demands on the platforms with which they communicate.

## 2 Background

The following properties are required of computing and transactions for trusted computing (TCPA, 2002a):

- **Trusted:** Does what it is supposed to do and can declare what it is supposed to do.
- **Reliable:** Available when needed, can take actions against threats to its availability.
- **Safe:** No unauthorized and potentially harmful operations are allowed.
- **Protected:** Information is shared with authorized parties only.
- **Private:** Users control their privacy.

The list above shows that the term “trusted computing” comprises many aspects. It is worth noting that according to the listed items, privacy is included and is not seen as something that lies outside the scope of trusted computing.

### 2.2.3 Important Terms and Entities in TCPA/TCG

The *Subsystem* is the isolated system that is trusted to work as it should since it cannot be tampered with, and it is the core of TCPA/TCG. Identity and integrity are assured through credentials, which are obtained through the usage of a Public Key Infrastructure (PKI) (TCPA, 2001). The purpose of the TCPA/TCG Subsystem is to make sure that the client is trusted by measuring and reporting *integrity metrics*, which are defined as “*measurements of key platform characteristics that can be used to establish platform identity, such as BIOS, boot-loader, OS loader, and the OS security policy*” (TCPA, 2000, p. 4).

The TCPA (2001) writes that the Subsystem capabilities (functions) are divided into two parts depending on whether or not they affect its trustworthiness:

- *Trusted Set (TS)*: The capabilities that are vital for the trustworthiness of the Subsystem, i.e., if any of these are not trustworthy, then the Subsystem as a whole is not trustworthy.
- *Trusted Support Set (TSS)*: The capabilities that do not influence the trustworthiness of the Subsystem, although they of course have to operate as intended for the Subsystem to operate as intended.

## 2 Background

The TS can be divided into a number of subcomponents (TCPA, 2001):

- *Root of Trust for Measurement (RTM)*: The measurement capabilities.
- *Root of Trust for Reporting (RTR)*: The reporting capabilities.
- *Root of Trust for Storage (RTS)*: The storage capabilities.

The RTM contains, among other things, the *Core Root of Trust for Measurement (CRTM)* which is where the computer starts executing in the trusted state (TCG, 2003b). The results of the measurements made by the RTM are given to the RTR, which protects the results from alteration and reports them when they are requested (TCPA, 2001). Thus, it is the RTM and the RTR that together provide the information about the computing environment in the platform, and this information is then used by other entities to judge whether the platform is to be trusted or not. The RTR uses a cryptographic identity to ensure that the messages it sends are not the result of fraudulent activity (TCPA, 2001). Even if the identity does not include all the trusted capabilities, it still works if trust is indirect. If an RTR with a certain identity belongs to a specific platform, then that platform contains the other trusted capabilities as well (this requires a statement from a trusted authority that the platform does indeed contain those trusted capabilities) (TCPA, 2001).

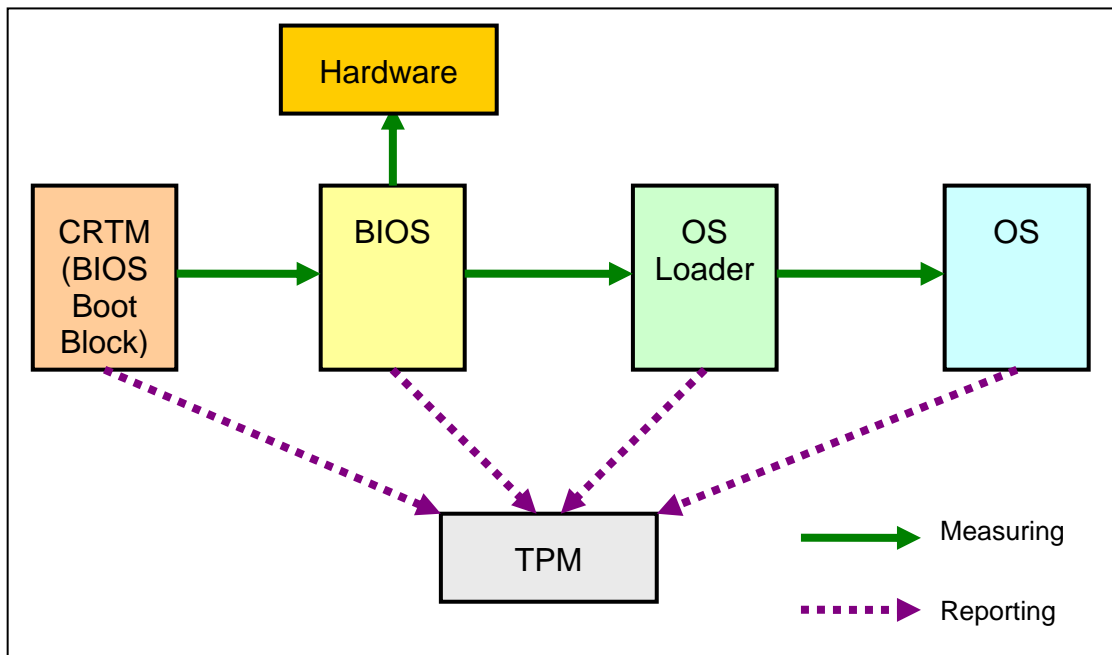
*Trusted Platform Module (TPM)* is a term used for all the trusted capabilities, excluding the RTM (TCPA, 2001). These capabilities are those that are the same for all trusted platforms (the RTM may differ depending on what platform it is implemented on). The TPM uses cryptography to identify itself and to report the measurement results (TCPA, 2001). This means that it is possible to identify each TPM uniquely. The TPM works together with specific software to achieve the aims of the specification (TCPA, 2000).

### 2.2.4 How Does It Work?

In the text below it is assumed that the platform is a PC. Even though TCPA/TCG is designed to be platform-independent, it has thus far been worked out primarily for the PC platform. These examples are provided to convey the general idea of TCPA/TCG.

The boot procedure of a TCPA/TCG-compliant PC would begin with assuring that the BIOS can be trusted. This is accomplished through a dialog between the TPM and the TCPA/TCG-compliant part of the BIOS. After that, the BIOS engages in a dialog with the operating system loader and the TPM to ensure that the operating system loader can be trusted. When the operating system loader is trusted, it "talks" with the operating system kernel. (The operating system kernel is defined by Pfleeger [1997, p. 292] as "*the part of an operating system that performs the lowest-level functions [...] such as synchronization, interprocess communication, message-passing, and interrupt-handling.*") Starting with the loading of the operating system kernel, everything that now takes place is under the supervision of the kernel (TCPA, 2000). This procedure is described graphically in Figure 2.

## 2 Background



**Figure 2.** Integrity measurements and storing of measured values during a PC's boot process. (After TCPA, 2001, p. 18.)

Trust is extended from the TPM all the way up to the applications. The basic idea is that the lower level assures that the level above it can be trusted, and then that level assures that the next level can be trusted, and so on. In other words, "*the initial point of trust (TPM and BIOS) spreads the trust throughout the whole system, thus resulting in a Trusted Client*" (TCPA, 2002c, p. 2).

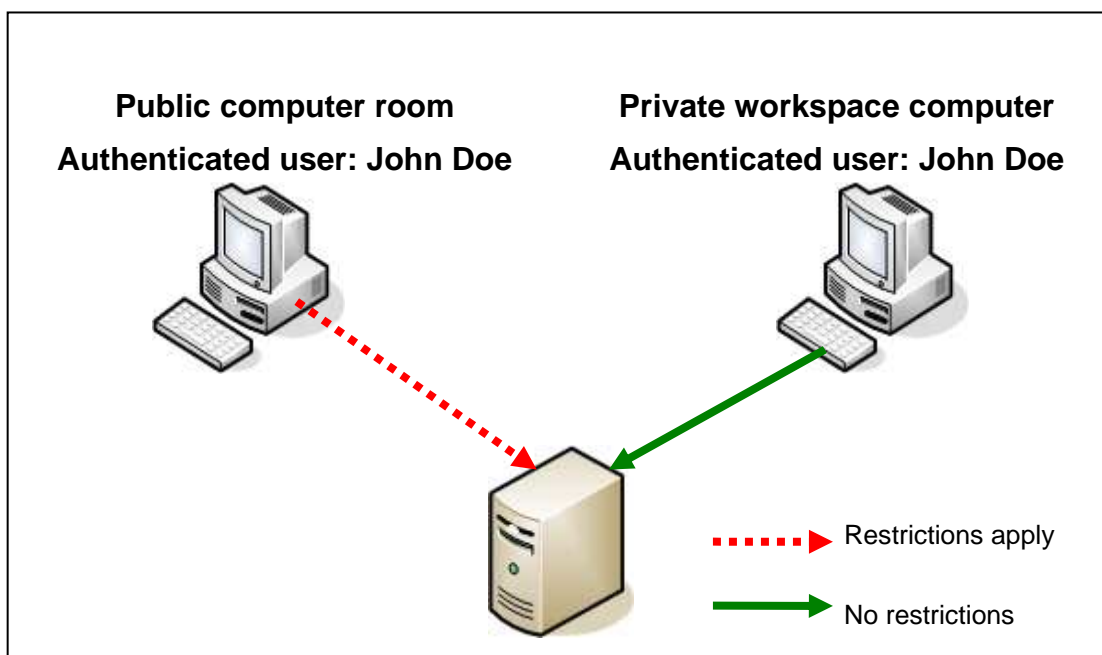
Data can be securely *sealed* (encrypted) using a key that is tied to a specific integrity metric of a computer (TCPA, 2001). This can be used to ensure that data sealed on one computer can only be *unsealed* (decrypted) on that same computer, and then only if the platform configuration is the same as it was when the data was encrypted. The latter means that data sealed under a certain operating system cannot be unsealed under a different operating system even if that other operating system runs on the same computer, and data sealed on one computer cannot be unsealed on another computer.

The following is a simplified example that describes remote attestation. Suppose that a user wishes to watch a streamed movie on his/her computer. The application that is used to watch movies sends a request to the movie provider's server. The server needs to make sure that the client complies with the policy that the provider has set for the client to be able to download the movie. Consequently, the server sends a request to the client for its integrity metrics. Upon receipt of the request, the client signs the integrity metrics digitally and sends them to the requesting server. The digital signature has two purposes: it makes sure that the integrity metrics cannot be tampered with during transmission and it allows the receiver to verify that the signature belongs to the client that it claims it comes from. Now, assuming that the signature was authentic, the server determines if the client is trustworthy by

## 2 Background

examining the received integrity metrics and comparing them to the integrity metrics expected from a client that is trustworthy according to the definition of the content provider. If the client proves to be trustworthy, the server sends the movie to the client. There is no judging of the integrity metrics involved in TCPA/TCG; it merely reports the integrity metrics and leaves the judging of trustworthiness to the requesting entity (TCPA, 2000; 2002e).

Related to remote attestation is the ability to authenticate a platform and/or user (TCPA, 2002a). The former allows remote parties to make sure the system with which they are communicating can be trusted, and the latter is a means for secure user authentication. With traditional user authentication it is the user credentials (i.e., user names and passwords) that decide what can and cannot be done. TCPA/TCG takes this further by making it possible to ensure that only users logged on with certain user credentials *and* working from certain computers can (or cannot) perform certain operations. If a user logs on using what is considered an insecure computer within an organization (e.g., from an open computer room at a university) certain sensitive operations cannot be performed, but when the same user logs on using a secure computer (e.g., his/her workplace computer located in a locked room) those operations can be performed (see Figure 3). The user credentials can thus be securely tied to the specific computer that is used, and different restrictions can apply depending on what computer is used.



**Figure 3.** It is possible to apply different restrictions on the same authenticated user depending on the computer that the user is logged on to and using. Here the restrictions concern operations on a server.

### 2.2.5 Summary

The TCPA/TCG was formed to develop a specification that would infuse trust into the world of computers. Since software is not sufficient to keep up with the demands of an increasingly digitalized and networked world, hardware is used to provide a solid foundation upon which software can then be verified for trustworthiness. TCPA/TCG requires some changes to the hardware and to certain software applications in order for it to work. It is through the cooperation between hardware and software that a system's components can be verified against certain values that would be expected for a system that is trustworthy for the intended usage. The system is considered trustworthy if the reported values match the expected values.

### 2.3 NGSCB

This section gives a description of Microsoft's NGSCB project and related terms and concepts. Like TCPA/TCG, NGSCB aims to provide secure computing and protection of privacy. However, while TCPA/TCG is primarily about ensuring that computer systems can be trusted, NGSCB strives to be a secure computing environment, including security measures on the local machine, such as encryption of information traveling from the graphics card to the monitor or from the keyboard to the motherboard.

NGSCB was originally called Palladium, but that code name has since been discontinued in favor of the current name because the new name describes what the project is about, and because Palladium is a non-Microsoft trademarked name (Dudley, 2003; Lettice, 2003). Regardless of this, the project is widely known as Palladium; therefore, that name will appear in some of the references.

#### 2.3.1 What Is NGSCB?

NGSCB is the name of a number of Microsoft-developed components designed to provide a secure foundation for computers (Carroll, Juarez, Polk, & Leininger, 2002). To take full advantage of NGSCB a new generation of hardware and software designed with NGSCB in mind must be used because current hardware and software cannot take advantage of the new technology. In relation to this, it is important to note that this does not imply that existing hardware and software will be useless. As Carroll et al. (2002) note, non-NGSCB hardware and software must also work on a NGSCB-enhanced computer. The difference is that current hardware and software cannot live up to the standards required for NGSCB. That is why a new generation of hardware is needed and why new software needs to be written or current software rewritten to take advantage of the NGSCB features. However, Microsoft is expecting a gradual shift over to NGSCB-enhanced systems; the corporation does not expect that all systems will be upgraded immediately (Microsoft, 2002).

## 2 Background

Since Microsoft is a member of the TCPA/TCG, NGSCB obviously has many similarities with it as it is based on that specification. However, NGSCB is not, according to Microsoft (2003c), merely an implementation of TCPA/TCG. The main difference is that NGSCB has a wider range of functionality than TCPA/TCG has: the latter focuses on attesting trustworthiness while the former is a more general approach to secure computing.

Carroll et al. (2002) write that NGSCB is supposed to provide the following:

- Higher security of information.
- Better protection of users' privacy.
- A guarantee of a system's integrity.

These features are provided through a trusted execution subsystem, which is the result of the combination of new hardware and enhancements made to the Windows operating system.

### 2.3.2 Important NGSCB Terms

The features of NGSCB can be divided into two types: hardware and software. The hardware part consists of the following:

- *Security Support Component (SSC)*. The SSC can be thought of as the hardware brain in NGSCB and corresponds to the TPM in TCPA/TCG. Microsoft (2003c) states that the SSC performs encryption, decryption, generation of digital signatures, and verification based on asymmetric cryptography (one key for encrypting and one key for decrypting). It is also responsible for encryption and decryption based on symmetric cryptography (one key for both encryption and decryption), and for hashing. The SSC must contain at a minimum one private key of a key pair (asymmetric) and a symmetric key that never leave the chip (Microsoft, 2003c).
- *Attestation*. The mechanism by which users can allow other entities to obtain certain knowledge of the platform environment (Microsoft, 2003a). (This feature is shared with TCPA/TCG.)
- *Sealed storage*. Some data can be stored in a way that makes it inaccessible to all programs except the one that sealed the data running on the same system as the data was sealed under (Microsoft, 2003a). This means that the sealed storage cannot be accessed from another operating system or if the physical hard disk is inserted into another machine. (This feature is shared with TCPA/TCG.)
- *Strong process isolation*. Achieved by adding a mode bit to the central processing unit (CPU) to distinguish between standard and trusted mode, and by allowing a portion of the random access memory (RAM) to be accessed

## 2 Background

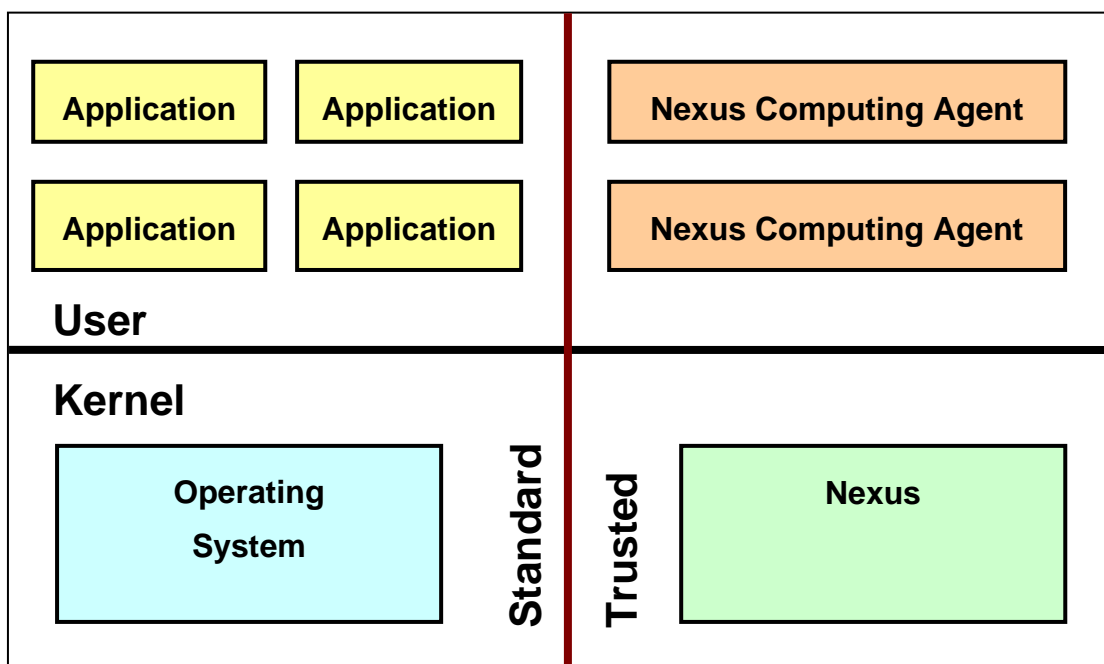
only when the CPU is in trusted mode (this is known as *curtained memory*) (Microsoft, 2003a). No software running in standard mode—including the operating system—can access information in the trusted memory areas.

- *Secure input and output.* Data traveling, for example, between the keyboard and the motherboard (keystrokes) or between the graphics processing unit (GPU) and the monitor (the image displayed on the monitor) is cryptographically protected so that it cannot be intercepted and picked up by unintended parties (Microsoft, 2003a).

The software part consists of the following:

- *Nexus* (formerly known as the Trusted Operating Root, TOR). The software supervisor. It handles the NGSCB functionality on the software side by providing services that trusted agents use. The nexus operates in kernel mode (as opposed to user mode) in the trusted space. The nexus can be thought of as the software brain in NGSCB. Microsoft (2002) says that the source code of this vital component will be published openly so that it can be scrutinized and verified by external parties (doing this will not in any way endanger the security of the component).
- *Nexus Computing Agents (NCAs) or trusted agents.* User-mode software that executes in the trusted environment (Microsoft, 2003a). They can be programs, parts of programs, or services. Security sensitive operations must go through the nexus. A trusted agent need not be considered trusted by all entities; rather, an agent that is trusted from the viewpoint of one entity is not necessarily trusted from another entity's viewpoint (Carroll et al., 2002).

NGSCB introduces a strong isolation between the traditional computer system and the new features that NGSCB adds. This isolation between standard and trusted mode can be seen in Figure 4.



**Figure 4.** The vertical line represents a hardware- and software-based isolation mechanism. To the left of the line are the traditional components of a computer system and to the right are the basic features of NGSCB. (After Microsoft, 2003b, p. 1.)

### 2.3.3 How Does It Work?

Microsoft plans to let NGSCB be an opt-in system (Carroll et al., 2002). This means that users actively must choose to enable NGSCB since NGSCB-enhanced systems will have the NGSCB functionality turned off by default. To ensure that no software can enable NGSCB if it is currently disabled, NGSCB can be completely turned off at the hardware level, which makes it impossible for software to enable it. It does, however, seem likely that if trusted computing ever becomes widespread, many applications and services will require that it be enabled; users are thus faced with a Hobson's choice.

A NGSCB-enhanced PC arrives at a trusted state through a process known as *authenticated startup* (Microsoft, 2003a). During this process the nexus is started and enables hardware and software to can be authenticated; the nexus itself is authenticated during the boot process. It is important to note that the SSC and the nexus are not part of the boot process; they are initiated when the user requests NGSCB services, and this can happen any time after the computer has booted (Microsoft, 2003c).

Computing devices and software can verify that other computing devices and software applications can be trusted by means of attestation (see section 2.3.2) (Carroll et al., 2002). This is important in many situations, such as when accessing financial services. When a server wants to assure that the client with whom it is communicating can be trusted, it sends a request for information about the client's current state to the client. The client responds with the required information, and based on the received information the server decides whether or not the client can be

## 2 Background

trusted. Additionally, both parties can be certain of the other party's identity, and they can communicate securely with each other.

Encryption is performed with secrets that are unique to each system, which means that encrypted information is useless if copied to another system or if the storage medium (hard disk) is stolen (Carroll et al., 2002). The secrets are protected through both physical and cryptographical means. Since the secrets reside in the hardware, no malicious software can gain access to them without going through the nexus, which will ensure that only trusted software is allowed to pass. In the event that these hardware secrets are revealed, they can only be used to compromise the system to which they belong. Therefore, if the secrets of one system are revealed, it does not mean that all NGSCB-enhanced systems are in danger; only the compromised system is.

Encrypted data can be migrated between computers and cryptographical keys can be backed up in case of a hardware change or failure, but no details outlining this process are available (Microsoft, 2003c). A third party must likely be involved, because if users could migrate NGSCB-encrypted data freely, what would stop them from migrating such data for the purpose of illegally distributing it? In any case, hardware changes and failures are not overlooked.

The user can create different *realms of data* (Carroll et al., 2002). These realms have their own identifiers and policies, and therefore allow users to set up for example one realm for financial information, one realm for confidential documents, and one realm for everything else. This separation can be seen as a number of vaults containing different items (Carroll et al., 2002). This makes it possible, as Carroll et al. (2002) point out, for users to have one part of the system protected while simultaneously having a completely open part. In other words, NGSCB-enhanced software can work with protected data while at the same time a Web browser is run in an adjacent window, since the open environment cannot interfere in any way with the protected environment because such interference would have to go through the nexus, which would not allow it to pass.

With NGSCB it will be possible to establish *closed spheres of trust* (Carroll et al., 2002) which are related to the concept of realms described above. The purpose of a closed sphere is to define under what circumstances that a particular protected area may be unlocked (that is, when the recipient can be trusted). Carroll et al. (2002) describe how this is accomplished: data or services are associated with one or more authorized users and with the applications that are allowed to access the data or service. It is therefore possible to unlock one specific closed sphere that contains the data that is needed in a certain situation. There is not one area that contains all data to be protected, and if that area is unlocked all protected data is available; rather, the user can unlock a certain closed sphere when doing operations that are related to the data in that sphere, while data in the other closed spheres are still protected.

## 2 Background

Secure and insecure windows will not look the same:

*“A non-writable banner with a trusted icon and program name appears on the top of each trusted window. The trusted window cannot be covered by other windows for programs that are running in the standard operating system environment. If more than one trusted window is open on the desktop, they do not overlap.”* (Microsoft, 2003a, p. 11.)

This makes it easy for users to distinguish between secure and insecure windows so that for example secret information is not entered into an insecure window. In addition to the visual difference the two types of windows behave differently

### **2.3.4 Summary**

NGSCB is a project that is being developed by Microsoft. It has certain similarities with TCPA/TCG, but NGSCB has some features that do not exist in TCPA/TCG, such as protection of intrasystem communication. A trusted area of the system is established, and all requests to access and/or manipulate data in the trusted area must go through the controlling software (called the nexus) that verifies the requests according to certain criteria and, depending on whether or not the verification was successful, grants the requests access. This approach isolates trusted applications and data from the rest of the system environment for maximum security.

## 3 Problem Description

The purpose of the dissertation is described in this chapter. The problem that will be presented, analyzed, and discussed in this dissertation is stated, and motivation is given as to why this problem is important and worthwhile to pursue.

### 3.1 Problem Specification

The overarching question is whether the positive sides of TCPA/TCG and NGSCB outweigh the negative sides; in other words, whether trusted computing must necessarily be disadvantageous for users or if it is possible that the technology could benefit them. This dissertation is primarily concerned with the following issues:

- What are the benefits of TCPA/TCG and NGSCB for users? For what could trusted computing be used beneficially?
- What are the risks with TCPA/TCG and NGSCB for users? How could trusted computing be used to cause damage to users?
- Why are TCPA/TCG and NGSCB criticized? Is the raised criticism valid, and can it be answered?

Other issues connected to those above will be brought up and discussed where appropriate, and a discussion in more general terms will be given in Chapter 7.

### 3.2 Motivation

TCPA/TCG and NGSCB are solutions proposed to address the increasing need for high security and trust that exists, and they should also safeguard users' right to privacy by protecting personal information. Both initiatives include means to protect the privacy of the users without neglecting the security aspects.

It is likely that TCPA/TCG, NGSCB, another similar initiative, or a combination of them will become a reality in a not-too-distant future. For that reason, an analysis of how the two currently existing initiatives have approached the issues of security and privacy from a viewpoint of the users is of interest. Such an analysis would serve to clarify what the benefits and risks of the two systems are. When systems like TCPA/TCG or NGSCB are fully deployed, it is important to be aware of the implications they will have in the areas of security and privacy so that none of them come as a complete surprise. It is better to discuss this now, when TCPA/TCG and NGSCB are under development and it is not too late to offer suggestions and convey comments and opinions to the developers.

Criticism can serve an important purpose by making people aware of things that the proponents either do not talk much about or do their best to hide. As in any process with profound implications for a large number of individuals, companies,

### 3 Problem Description

organizations, and governments, it is important that as much information as possible—both positive and negative—is given to those who make the decisions and to those that are affected by the decisions. In doing so, well-informed decisions can be made and actions taken. By ventilating criticism at this stage, it is possible that the organizations behind TCPA/TCG and NGSCB heed these negative opinions and do their best to try to amend the issues that are criticized, given that the raised criticism is valid.

Furthermore, it is important to see if the criticism that is raised can be answered. It is important to filter out valid criticism from criticism that stems from misunderstandings or is raised without any justifiable grounds just for the purpose of criticizing. Therefore, possible answers to the criticism will be included in the analysis.

#### **3.3 Purpose**

The dissertation aims to analyze and discuss the advantages and disadvantages that TCPA/TCG and NGSCB will bring to users in the areas of security and privacy. Do TCPA/TCG and NGSCB live up to the promises that the proponents have put forth? Is the criticism right in all its claims?

The information available from the organizations that have developed TCPA/TCG and NGSCB will be set against some of the criticism that has been raised against the two systems. The purpose of this is to see where the critics may be correct in their arguments and where they may be wrong. What are the arguments that are put forth by individuals and organizations that criticize TCPA/TCG and NGSCB? Is it possible that some of the criticism is incorrect, whether by mistake, insufficient knowledge of the details, or perhaps intentionally? Is it possible to state, from the results that have been obtained, the benefits of and risks with the two systems for users?

This is done in an attempt to evaluate trusted computing from the perspective of the users. Is trusted computing something that users should fear or is it something that they should welcome?

#### **3.4 Expected Result**

The expected result of this dissertation is to show that even though TCPA/TCG and NGSCB include features that could potentially lead to unwanted consequences, the two systems offer a number of features that are welcome efforts to make the currently insecure, networked world more secure. It is while TCPA/TCG and NGSCB are still in development stages that the public must be made aware of the features of the two systems, their advantages and disadvantages, and the implications that they will have once they are introduced and available on the market.

## 4 Method and Approach

This chapter contains a brief discussion concerning how the problem will be approached and analyzed. Issues regarding the references, such as quality and bias, will also be brought up.

### 4.1 Method

Due to the nature of the issues that this dissertation deals with, the adopted approach is literature studies. There are issues with basing a dissertation on literature studies, just as there are issues with other approaches as well. In the case of this dissertation, literature studies are the most appropriate approach for reasons explained above.

The dissertation will be based on published, printed articles and books whenever possible. Since TCPA/TCG and NGSCB are systems that are under development there are limits as to the amount of material written and published in print about these systems. Due to the lack of sufficient printed material, many of the references pertaining to the two systems come from sources available on the Internet where details about TCPA/TCG and NGSCB are available as soon as they become publicly known. There is plenty of information on TCPA/TCG and NGSCB available on the Internet, and the reason for this is that the systems in question are highly controversial and tend to evoke some kind of opinion in everyone who has at least some basic knowledge of what TCPA/TCG and NGSCB are about.

The quality of the information available on the Internet varies very much, and therefore the references used in this work have been selected because they come from high-quality, trusted sources that can be assumed to publish information that is correct, true, and verified. Furthermore, the information must not contain any claims that cannot be verified or at least assumed to be correct based on information available from other trusted sources. Sources that meet these requirements include the TCPA/TCG and Microsoft, The New York Times on the Web, and The Register. Names such as these are taken to be guarantees for the quality and correctness of the information that is published. Individuals that provide information should be known to be somehow involved with TCPA/TCG or NGSCB (proponent or opponent) or be able to show that his/her information is supported by other high-quality, trusted sources.

Much of the information about TCPA/TCG and NGSCB will be taken from material published by the TCPA/TCG and Microsoft respectively. Clearly, some of this information will be biased; however, the formal specifications can be regarded as less biased than more informal information such as brochures and documents with questions and answers. The reason for that is that the specifications are meant to give detailed technical information about the standards; hence, they do not contain much informal text, and if they do, that text is clearly marked as being informal. Furthermore, since the TCPA/TCG is an organization consisting of many member companies, it is important to be aware that any information on TCPA/TCG from the

## 4 Method and Approach

organization's members is likely to be biased. The same goes for critical information as well, which is likely to be biased toward the other side in much of what is written.

### 4.2 Approach

The work commenced with the decision to search the Internet for as much relevant information as possible in the following categories:

- Information about TCPA/TCG and NGSCB from the developers (the TCPA/TCG and Microsoft).
- Information about TCPA/TCG and NGSCB from sources other than the developers.
- Information with a positive view of TCPA/TCG and NGSCB (not including the developing organizations).
- Information with a negative view of TCPA/TCG and NGSCB.

The search for information was divided into three parts based on the above categories. First interesting information was gathered from the TCPA/TCG and Microsoft. The next step was to find information from other Internet sources, such as online newspapers and magazines. The third part was finding specifically positive and negative information about TCPA/TCG and NGSCB. There are many texts available on the Internet criticizing TCPA/TCG and/or NGSCB; in fact, negative information was easy to obtain, while acquiring information with a positive stance toward TCPA/TCG and/or NGSCB required a bit more effort.

The printed material used in this dissertation provided general information on topics closely related to TCPA/TCG, NGSCB, and other important concepts and terms discussed herein. Printed material has been used to support non-print sources whenever possible, but in most cases this was not possible for reasons explained in Section 4.1. Therefore, the Internet was the largest source of information. Care has been taken to use sources that were deemed generally trustworthy and correct in order to ensure the quality of the information.

## 5 Analysis

This chapter presents possible benefits of TCPA/TCG and NGSCB, as well as criticism that has been raised against the two systems. Much of the criticism against the two systems stems from the fear of losing the freedom of choice and control over one's own computers; therefore it is natural that the focus will be on those areas. In addition to this, possible answers to the raised criticism will be given.

### 5.1 TCPA/TCG and NGSCB Benefits

The features of TCPA/TCG and NGSCB were described in Chapter 2, and it should be clear that TCPA/TCG and NGSCB are able to provide very high security in various ways in a number of different areas. Some possible applications of trusted computing will be brought up in this section in order to show that trusted computing can be used beneficially for things that users care about.

It is difficult to find information that pertains to uses of trusted computing that users would benefit from. Some possible applications are brought up in the material from the developers, but these are only a small part of the areas in which trusted computing could be used. One possible reason for the seeming scarcity of information on positive uses of trusted computing from sources not directly involved in the development of said technology may be that it is easier to find and discuss the extreme risks than it is to do a thorough analysis of the complexities of the issue in order to obtain the subtler nuances. Another reason may be that one probably receives more attention and publicity discussing the risks since trusted computing seems to have a negative connotation among the majority of users.

The most important feature of TCPA/TCG and NGSCB with respect to possible applications is remote attestation (see section 2.2.1) which is at the center of trusted computing since it allows clients and servers to be sure that their counterparts can be trusted, where trust is defined differently depending on the application. Sealed storage provides a means for storing data securely, and process isolation and secure input/output—NGSCB-only features—give further advantages.

Trusted computing could be used to combat spam and viruses (Microsoft, 2003c). The technology could be used to digitally sign e-mail or to ensure that some complex computation is performed before messages are sent (the latter would prevent spammers from sending thousands of messages per minute since the computation for each message may take something like 10 or 20 seconds). Users could then reject messages or treat them as spam if they are not signed or if the sender cannot prove that the required computation was actually performed.

When it comes to viruses, trusted computing could protect antivirus software from corruption, thus ensuring that it will always be able to detect and remove viruses (Microsoft, 2003c). Furthermore, viruses and other kinds of malicious software would

be unable to access and steal sensitive information stored securely by the means that trusted computing makes available (Safford, 2002).

*Online elections* would benefit from trusted computing since it would make it possible for the central voting server to ensure that all voters are running an authorized and unmodified version of the voting software (“Internet Voting, Safely,” 2004). Sensitive data related to the voting could be securely stored and would not be available even to the voter, something that would prevent vote selling. In the case of NGSCB, in addition to the above, no other software would be able to interfere with the voting software, and no other software would be able to intercept input (keyboard, mouse) or output (what is displayed on the monitor).

*Multi-player computer games* could be improved by trusted computing (“Interesting Uses of Trusted Computing,” 2004). Game servers would be able to ensure that all players are running an unmodified version of the game, which means that it would not be possible to cheat. Furthermore, data supposed to be hidden from the players can be kept hidden.

Trusted computing would greatly improve the *security of online financial transactions* by enabling the bank to make sure that the client can be trusted (“Interesting Uses of Trusted Computing,” 2004). Sensitive financial data can be securely stored, other software cannot interfere with the software through which the transactions take place (e.g., a Web browser or a dedicated banking software), and—with NGSCB—financial information displayed on the monitor cannot be intercepted by other software.

In *peer-to-peer (P2P) networks* (also know as file-sharing networks), users can ensure that other users are running authorized and unmodified versions of software (“Interesting Uses of Trusted Computing,” 2004). By protecting such networks from unauthorized and modified versions, the networks will be safer and stabler. Schechter, Greenstadt, and Smith (2003) have argued that if trusted computing lives up to its promises, then that technology will be able to protect peer-to-peer networks from attacks and make them safer and more reliable. Malicious client software would not be able to access the networks since remote attestation will prevent unauthorized software versions or authorized versions running on computers that cannot be considered trusted from using the networks. Furthermore, secure storage and curtained memory could be used to provide secure data storage and ensure that malicious software running on client computers cannot interfere with clients’ peer-to-peer software on the same computer (Schechter et al., 2003). Worth noting is that one of the persons mentioned in the “Acknowledgments” chapter of the paper is Ross Anderson, who has argued strongly against trusted computing, and also that the authors’ research was partly supported financially by Compaq, HP, IBM, Intel, and Microsoft, all of which are involved in the development of trusted computing.

*Distributed computing* (SETI@home and distributed.net for example) would be able to take advantage of trusted computing to ensure that client software is unmodified (“Interesting Uses of Trusted Computing, Part 2,” 2004). The data is modified to make the client process data faster and thereby get a higher ranking, but it makes the processed data useless for scientific purposes. The client’s data can be protected from modification by software other than the client itself.

Trusted computing could help *protect customer privacy* when shopping online (“Interesting Uses of Trusted Computing, Part 2,” 2004). Customers would be able to verify that shopping sites are using software approved for that use and is known to keep customer data private.

The above are just a few of the possible applications of trusted computing, and when trusted computing is widely available (assuming it will be at some point in time) many more ways of using this technology will be discovered. With more secure computers, there will be a number of novel things that we will be able to use our computers for, things for which computers thus far have been too insecure.

Critics could claim that all beneficial uses of trusted computing are just devised to direct attention away from the risks, or they may acknowledge that the benefits are real but that they are not proportionate to the risks. In any case, if the critics have decided that trusted computing is basically bad for users, then no amount of possible beneficial uses of the technology is likely to convince them otherwise.

### **5.2 TCPA/TCG and NGSCB Criticism and Replies to It**

The purpose of this section is to present and analyze criticism that has been raised against trusted computing. Possible replies to the criticism will also be considered. Focus will lie on digital rights management and user privacy.

#### **5.2.1 Digital Rights Management (DRM)**

The term “digital rights management” or “DRM” is used for hardware and software that make it possible for owners (copyright holders, content providers, etc.) to decide in what ways their material can be used by enforcing the policy set by the owners. This could for example be that a certain document cannot be printed or edited, or that certain music and video files can only be run by applications that are known to enforce the policies decided by the owners of those files. It seems likely that content providers would take advantage of whatever means are available for strong DRM systems, including trusted computing.

Critics, such as Anderson (2003), claim that the primary motivation for developing TCPA/TCG and NGSCB is DRM. With the strong DRM that TCPA/TCG and NGSCB make possible, the owners of copyrighted material such as music and movies could make sure that their material is used in the way that they want, and only in that way. There is a real potential for misuse and too restrictive policies, and fair use is threatened.

Question four in a document containing questions and answers (TCPA, 2002e): “*Is the real ‘goal’ of TCPA to design a TPM to act as a DRM or Content Protection device?*” (p. 1). The answer that is given is as expected negative. TCPA/TCG is about increasing trust in computer platforms. Therefore, it can be argued that TCPA/TCG is

## 5 Analysis

not about DRM, although it could possibly be extended for that purpose since it provides the basic functionality that a strong DRM system would require.

Microsoft (2003c) claims that NGSCB is not about DRM, but acknowledge that DRM would benefit from NGSCB. Therefore, while NGSCB provides a strong basis for DRM, it will also give consumers better security and protection of privacy (Microsoft, 2003c). Protection of, for example, movies or music works in ways similar to protection of personal information since what is protected in both cases is data. NGSCB does not make any distinctions between the data it protects: to the system, all data is the same, regardless of what it represents. Even if it were possible to exclude DRM entirely from NGSCB, Microsoft would most likely not do it, since NGSCB would then not be as broad as the corporation would like.

Microsoft has filed a patent regarding DRM (Orlowski, 2001; Loney, 2002). Loney (2002) speculates, based on the patent application, that even though NGSCB could be used for a number of purposes, it is primarily about DRM. Also worth noting is the fact that NGSCB emerged from work done by “*a small group of Microsoft employees who were working to solve the problem of content protection for online movies*” (Microsoft, 2002, p. 2). This provides an indication that DRM in some form is present at the heart of the thinking behind NGSCB.

Schoen (2003) discusses the use of trusted computing for DRM enforcement, and he acknowledges that DRM is just one possible use of trusted computing. The centerpiece of DRM enforcement, according to Schoen (2003), is remote attestation. The other features of trusted computing play important roles, but remote attestation is what allows DRM policies to be established. The importance of this will be clear later, in Section 5.2.5.

One thing to keep in mind is that widespread deployment of trusted computing does not automatically enable DRM. In addition to the part played by trusted computing, it will be necessary to set up the infrastructure for the DRM system, and this is something that will take time for content providers and other related parties to do (“EFF Report on Trusted Computing,” 2003). A considerable amount of work would have to be done by content providers wishing to use trusted computing for DRM systems. This is no argument against such use, but it does show that effective and secure DRM systems will not automatically follow from the implementation of trusted computing.

Safford (2002), an IBM researcher, has stated that he thinks that DRM can never be effective and that it removes consumer rights, but he does not see DRM opposition as a reason to oppose trusted computing altogether. The support trusted computing gives to DRM is not a reason for arguing that trusted computing is bad for users since all the good uses of trusted computing are not taken into account (Safford, 2002).

Bechtold (2003) writes that even though a DRM system based on trusted computing would be much more secure than current DRM systems, it does not mean that they

would be completely secure. He argues that it is not at all certain that trusted computing will even be used as a basis for DRM, and the reason for this is twofold. It does not provide very high security against attacks performed by the owner of the computer, and a DRM system based on trusted computing would be very complex due to the vast amount of different integrity metrics that would be reported (different hardware, different software, different versions of the same software, etc).

It should be no surprise that not even the DRM enabled by trusted computing is a completely secure solution. Schechter et al. (2003) write: “*if humans are to eventually hear the protected audio signals and view the protected video signals, then this protected content can also be recorded*” (p. 5), and this is echoed in the document “DRM is Great, But It Won't Work” (2004). The author of that document also writes that DRM can at best prevent more people from using or distributing material illegally than is possible with no DRM system at all, but it cannot prevent everyone from doing so. Trusted computing would indeed provide much stronger DRM than what is possible today, but if someone with the right resources really wanted to circumvent the protection, it would be possible to do so in one way or another.

### 5.2.2 Privacy

No specific information on how privacy is protected in NGSCB is available from Microsoft, but since the privacy issues stem from the remote attestation feature that TCPA/TCG and NGSCB share, it seems reasonable to assume that the privacy-related information that applies to TCPA/TCG also applies to NGSCB.

The privacy implications of remote attestation should be easy to see. If every computer would be required to use the unique identity associated with the computer's TPM, it would not be very difficult to track that computer (and thereby possibly the user) whenever remote attestation is used. Each TPM contains a unique *Endorsement Key (EK)* that consists of a private key and a public key, and the EK is used to authenticate the validity of the TPM. When remote attestation is performed, the public part of the EK must be released from the TPM (TCG, 2003c). That would be devastating for privacy since both the private and public key of the EK are unique. TCG (2003c) writes that all TPMs must contain a unique EK because if all TPMs shared the same EK and one TPM were compromised, then all TPMs would in effect be compromised and could not be trusted.

The solution to this predicament was that computers would use the Endorsement Key only in interactions with a *Trusted Third Party (TTP)* (TCG, 2003c). A computer authenticates itself against a TTP, and the TTP generates a new key pair and sends it to the computer. This new key pair is called the *Attestation Identity Key (AIK)* and it ensures that the key holder has been validated by a TTP. It is that key pair that is then used in remote attestations with other parties. This means that other parties can only know that the computer on the other end has a valid TPM, but they never see the EK. This solution is certainly much better than exposing the public part of the EK to everyone, but the problem is that the TTP can identify the computer since it can associate the public part of the EK with the AIK it generated. To address this

## 5 Analysis

problem, the specification allows one computer to obtain many AIKs, one for each attestation if necessary (TCG, 2003c). User privacy is satisfied in this way unless the connection between the EK and the AIKs can be made.

The European Union Article 29 Working Party has written a report on trusted computing and the TCG, and has expressed an interest in receiving regular reports about the TCG's work (TCG, 2004a). The background to this report is that the Working Party analyzed the TCG's work from the perspective of European data protection laws. A number of concerns were brought up by the Working Party, and those concerns have been addressed by the TCG in the TCG TPM 1.2 Specification (TCG, 2004a). One of the concerns of the Working Party was that the benefits of trusted computing for consumers are not as obvious as the benefits for companies and organizations. The TCG's response to this was that there are benefits for consumers and that more education of consumers is necessary for them to see the benefits (TCG, 2004a).

It is worth spending some time on the new privacy-related features in version 1.2 of the TCG TPM specification to show that there is an interest in protecting user privacy. The most important feature is *Direct Anonymous Attestation (DAA)*, which is a way of generating AIKs without the need to release the EK, and in addition to this, computers can engage in direct attestation without going through a TTP (TCG, 2003c). To use DAA, a set of DAA credentials must be generated by the TPM. In the words of the TCG: "*The DAA-credentials are generated in an interaction between the TPM and the Issuer using a TPM-unique secret that remains within the TPM. This TPM-unique secret is used in every DAA-credential, and is: distinct from, but analogous to, the EK*" (TCG, 2003c, p. 5). Other parties ("Verifiers") can then determine "*if the TPM contains a valid set of DAA-credentials from a particular Issuer, but does not have specific knowledge of identifying the TPM from among others that also have valid DAA-credentials*" (TCG, 2003c, p. 5).

The level of privacy that DAA gives is determined by a variable called the "Base" (TCG, 2003c). If a random value of that variable is used for every verification, DAA gives complete anonymity, but if the same value is always used, Verifiers can identify TPMs if they verify themselves against the same Verifier more than once. So why not include a random-number generator in the TPM and use that to determine the value of the Base for each verification? Doing so would make verification meaningless since a completely random value of the Base would be tantamount to using one global EK for all TPMs (TCG, 2003c).

The *Named-Base solution* has been developed to solve this issue, and the idea is that the value of the Base that is used by a Verifier remains the same for some time before the value is changed. This allows Verifiers to "*detect repeated verification attempts by a real or cloned TPM using the same DAA-credentials*" (TCG, 2003c, p. 6). The point is that if a TPM's DAA credentials were somehow compromised and used in cloned TPMs, all those TPMs would use the same value of the Base; i.e., the Verifier would see more than one TPM trying to verify themselves using the same DAA credentials. Regarding anonymity, TCG (2003c) writes:

*“If each Verifier uses a distinct Named-Base and the interval between Named-Base changes is short, then the DAA protocol achieves nearly perfect anonymity. In particular, if a TPM approaches a Verifier only once during the interval of a given Named Base the system provides the same anonymity for that TPM user as if a random Base was used.”* (p. 7)

*Delegation* is another privacy-related feature that allows the system owner to grant software access only to certain TPM commands and not to the entire set of such commands, thus making it possible for software to use certain commands without the owner password and only allowing trusted software to execute privacy-sensitive commands (TCG, 2003c). The other new features concerning privacy are *Non-Volatile (NV) Storage* (basically an extension of protected storage), *Transport Protection* (allows the TPM and trusted processes to communicate securely), and *General Purpose I/O Function* (provides secure communication between the TPM and other hardware installed in the computer) (TCG, 2003c).

The author of “EFF Report on Trusted Computing” (2003) writes that there is a risk that the companies involved in trusted computing will fail to find a satisfactory solution to the privacy issue due to its complexity and therefore allow user privacy to be compromised. Clearly, the new features of version 1.2 of the TPM specification discussed in the last few paragraphs above are privacy positive and a great improvement over the earlier version 1.1b specification. The organizations working on developing trusted computing seems to have listened to and addressed the issues raised by various groups, something that becomes apparent if a comparison is made between the privacy-protecting features of version 1.1b and version 1.2 of the TPM specification.

### **5.2.3 Anti-Piracy Systems and Remote Censuring**

It has been suggested that TCPA/TCG and NGSCB could be used for anti-piracy purposes (Anderson, 2003; Microsoft, 2003; TCPA, 2002e). The idea is that TCPA/TCG- and NGSCB-enabled systems will be able to find and delete pirated software. One example of this would be that if a user tries to run a pirated program, the operating system would be aware of this since applications must be validated against a central server before they could execute, and the pirated program would not be allowed to run and it might even be automatically deleted. This, however, would go against the important part of TCPA/TCG and NGSCB that says that the system owner will have complete control over his/her system and that no action will be taken that goes against the owner’s wishes (TCPA, 2002e; Microsoft, 2003).

The TCPA (2002e) states that “*the TPM is a passive device*” (p. 1) and that “[*t*]he *TMP is not intended, nor is it sufficient for anti-piracy systems*” (p. 2), and Microsoft (2003c) writes that there will be no anti-piracy features in NGSCB. There is nothing in the current specifications that allows for remote deletion of software or remote validation of individual software registration keys, albeit Safford (2002) notes that it could theoretically be done. The TPM is a passive device and performs tasks only when it is asked to; it is not actively monitoring what goes on in the computer. Therefore, there would be no problem running pirated software of today; however, it

is possible for future software to be written to take advantage of the new features of trusted computing, and that would make running illegal copies of such software much more difficult (Microsoft, 2003c).

Related to the above is remote censoring. Schoen (2003) describes a case of such censoring. A program could be written to use a revocation list from some authority. If the program is a document viewer, the revocation list may contain documents that the viewer is not allowed to open. It would be possible to revoke documents long after they have been distributed, and even if users have for example downloaded them to their own computer from the Internet (Schoen, 2003). This would clearly be a very effective censoring, and it would certainly have devastating implications. Just as in the case of anti-piracy systems, there is no such functionality in the current specifications, but it is something that should be kept in mind as it is not a wholly unrealistic scenario.

### **5.2.4 Open-Source Software and Lock-In Scenarios**

There are critics, such as Ross Anderson (2003) who say that TCPA/TCG and NGSCB can pose a big threat to open-source development. As the argument goes, all software wishing to run on TCPA/TCG- and NGSCB-enabled systems must be certified. Furthermore, with TCPA/TCG and NGSCB companies can make sure that their proprietary file formats cannot be read by any other application than their own. This would prevent for example files created with Microsoft Word to be opened with competing products such as Sun Microsystems' StarOffice or the free OpenOffice.org (Anderson, 2003). A similar scenario is given by Bechtold (2003), though he gives a more nuanced and objective account.

As Safford (2002) points out, there is no requirement of code validation in trusted computing. Anyone can write programs that use the features provided by trusted computing, and no certification or validation of such code is necessary ("EFF Report on Trusted Computing," 2003). The user, and no one else, decides what software runs on the computer.

One of the questions concerns the possible development of a nexus for operating systems other than Windows, such as open-source operating systems (Microsoft, 2003c). The answer is that it is technologically possible, but Microsoft adds that there are issues with patents and intellectual property to consider. It is not entirely clear how this should be interpreted, but it seems to be the case that there would be issues to resolve before a nexus could be developed for alternate operating systems. In any case, this is something that only concerns NGSCB; it does not affect TCPA/TCG.

Anderson (2003), Bechtold (2003), and Schoen (2003) bring up problems with software interoperability. Imagine a scenario where a user has a lot of important information stored in files created with a certain program. That program could have been written to take advantage of the features of trusted computing to make it difficult or impossible to open those files with a product from a competing company. The

## 5 Analysis

hassle that would be involved in the migration of all the data to another file format may be too much work and too costly for the users, so they simply continue using the original software, even though the competing software for some reason may be preferable.

Trusted computing makes it possible for companies to enable lock-in that is virtually impossible to circumvent, and according to Schoen (2003) it is remote attestation that is the primary cause of this problem, with sealed storage playing a secondary role. There are, however, people that do not share this view. The author of the “EFF Report on Trusted Computing” (2003) writes that sealed storage is the primary feature involved in lock-in scenarios, since it only allows the program that sealed certain data to unseal it again. This difference is important since Schoen (2003) argues that remote attestation is bad; the other features of trusted computing are generally good. If it is sealed storage and not remote attestation that is the important feature in question as far as lock-in scenarios are concerned, as indeed seems to be the case, then it is not as simple a task as the EFF report makes it look like to draw a line between the bad and the good features of trusted computing.

In addition to software lock-in, Schoen (2003) discusses a different kind of lock-in that concerns the Web. Web sites might require visitors to use a certain Web browser, and if users try to access the site with a different browser, they will not be able to do so since remote attestation will reveal to the Web site that the users are not running the required Web browser. While this is perhaps a less likely scenario, the mere possibility of it should not be underestimated.

### **5.2.5 Owner Override: A Proposed Solution That Does Not Work?**

The last part of this criticism-and-replies section will be concerned with a proposed solution to eliminate some of the perceived risks with trusted computing. The solution is proposed by Schoen (2003) and comes in the form of an Owner Override.

One thing that seems to permeate criticism against trusted computing is that computer users lose some control over their own computer, and by including an Owner Override feature, it would be possible to retain complete control. Schoen (2003) writes that it is remote attestation that is the biggest worry, and the Owner Override is therefore related to that function. Here is a summary of the Owner Override:

*“Owner Override works by empowering a computer owner, when physically present at the computer in question, deliberately to choose to generate an attestation which does not reflect the actual state of the software environment -- to present the picture of her choice of her computer’s operating system, application software or drivers.”* (Schoen, 2003, p. 12.)

In other words, a computer owner can actually make the computer lie about the system state. Unauthorized changes can still be detected since generation of false

## 5 Analysis

attestations requires the active participation of the user. The point is that users should be able to conceal the voluntary changes a user has made on his/her computer. One is tempted to ask if it would be possible to guarantee that false attestations can be generated only by a user's active involvement. Is it completely inconceivable that a way of generating such attestations automatically could be found and exploited for malicious purposes?

Schoen (2003) claims that an Owner Override feature would not undermine the benefits of trusted computing, something which is criticized by the author of "EFF Report on Trusted Computing" (2003) who writes that such a feature *does* undermine remote attestation and render it useless. The whole point of remote attestation is that attestations should accurately reflect the current state of the computer, so allowing the computer owner to generate false attestations seems to decrease dramatically its usefulness.

While the Owner Override suggestion may or may not be an acceptable means for improving trusted computing for users, it is certainly positive that the suggestion has been made in the first place. Instead of immediately rejecting trusted computing and leave it at that, people like Schoen can contribute with valuable suggestions that, even though they may forever remain suggestions, could have a direct or indirect impact on the future work on trusted computing.

### 5.3 Summary

There are already at this stage examples of how trusted computing could enhance applications that are beneficial to users, and more are likely to be discovered as trusted computing develops. Some of the things that are criticized are based more on fear, speculation, and misunderstanding than on facts. Most of the valid criticism can be answered, or is otherwise not a reason for rejecting the whole concept of trusted computing. There are, however, valid points of concern as the two initiatives potentially could be used for other purposes than the intended ones.

Many critics claim that trusted computing primarily is being developed for software vendors, content suppliers, and the like, and not for greatly enhanced security and privacy for consumers. The situation is, however, not as simple as that. The reason for this is that it is the same technology that is applied in different ways. The technology that enables much higher security for users is the same technology that enables much stronger DRM systems, poses a threat to user privacy, makes technical lock-in situations possible, etc.

As has been discussed above, the developers of trusted computing have shown that they are willing to address user concerns; for example, the new privacy-related features of the TPM v1.2 Specification are not just for show; they actually enhance the protection of privacy.

### 6 Conclusion

The general benefits of TCPA/TCG and NGSCB are not very difficult to see. Services that exist today could greatly benefit from the increased security that would be the result of trusted computing. There may be services that are cumbersome for users to access or use due to extra precautions that have to be taken to ensure a sufficient level of security, and such services could potentially be made both securer and easier to use through the deployment of trusted computing. It is likely that new services will be developed that have previously been impossible due to the insecure computing architecture.

Trusted computing would not have been such a controversial subject if the story had ended there, but it does not. The same technology that is used to provide security in trusted computing could be used in various ways that would possibly be devastating for users. With trusted computing, it becomes possible to enforce strong DRM schemes that control what users can and cannot do with protected material. While many would perhaps not see anything inherently wrong with DRM, it is the same technology that could allow software companies to ensure that files created with their products cannot be opened with software from a competing company.

Another concern is that of user privacy. Solutions that allow privacy to be protected exist in the TPM specification, and they have been continually improving as concerns from various parties have been addressed. Other arguments against trusted computing have been shown to be pure speculation at this point in time: software will not require certification to work on or take advantage of the new features of TCPA/TCG- and NGSCB-enabled systems, and there exists no functionality for detecting and deleting pirated software. The same goes for remote censoring. Such functionality could, however, conceivably be implemented at a later stage. Arguments based on speculation have less force than those based on facts, but trusted computing should nevertheless be discussed not only in the short-term perspective but also in the long-term perspective.

Steps must be taken to ensure that trusted computing will never be used for malicious purposes, and they must not be confined to one area such as technology or politics; rather, a broad approach is needed. Even though no one may be considering using trusted computing maliciously as the situation looks today, once the technology is in place, such behavior might be very tempting.

It should be clear by now that TCPA/TCG and NGSCB are double-edged swords and that there is no way of getting away from that. Trusted computing can be used for good purposes and for bad purposes since it is the same technology that enables both types. We cannot have the good without the bad. What can be done is to ensure that the good effects of trusted computing are maximized and the bad effects minimized. Ultimately, it is the policies that are enforced that determine how trusted computing will be used, and this would be an interesting field of further study, addressing questions such as what policies give the best balance between the needs of users and corporations. There may come a point in time, however, when users, if they want the

## 6 Conclusion

advantages of trusted computing, must accept that the technology could potentially have some bad effects and that it does come with some disadvantages. One possible venue for future work would be to conduct a survey of user acceptance among people that are educated on what trusted computing is as well as its benefits and risks.

So, are users better off with or without trusted computing? Early in the development of trusted computing, it certainly looked as if the risks of the new technology outweighed its advantages, but things have changed for the better since then. The latest TPM specification (version 1.2) includes several new features for protecting user privacy, and these features are the result of feedback given on earlier specifications. Judging from the latest TPM specification, the TCG is committed to addressing user concerns regarding privacy and others issues, and this is a promising sign. It is not possible to evaluate fully trusted computing at this stage since the technology is currently in development, but a general conclusion based on the information that is presently available will now be attempted.

The advantages of TCPA/TCG and NGSCB in their current form are too good to be disregarded and simply abandoned. Therefore, the developers need to work hard to ensure that the worst fears of the opponents can never become true while at the same time making sure that none of the advantageous features of trusted computing are lost. User concerns should be addressed appropriately and timely, and the organizations involved in the development of trusted computing should make an effort to minimize potential risks and to educate users on what the technology is about so that the discussion does not hinge on misinformation or misunderstandings. If this is done, then users should be able to adopt trusted computing and enjoy its advantages without having to fear its disadvantages.

## 7 Discussion

One thing that merits discussion is the fact that Microsoft was a founding member of TCPA and later TCG, but the corporation is at the same time working on a project of its own. One might wonder why Microsoft is not simply working to bring the additional features of NGSCB within the framework of TCG. The answer is likely that the work of the TCG is meant to be broad, applying to a wide range of computing devices. The additional features of NGSCB essentially concern PCs only and are therefore of little interest to the TCG; the organization provides a general framework and individual corporations are free to add further enhancements to specific implementations based on the TCG specifications.

DRM is something that is widely discussed. What makes it controversial is that it can be used to restrict what users can do with things such as audio and video files that are in their possession, the restrictions being imposed by for example the copyright holder or the content provider.

At first glance, DRM may seem perfectly reasonable. Of course copyright holders should be able to control how their material is used, and of course movie makers, record labels, software developers, etc., are entitled to make sure that their products are not illegally copied and distributed against their wishes and without their getting paid for the work that has gone into these products. (The document “DRM is Great, But It Won't Work” [2004] discusses something along these lines.) However, as Loney (2002) notes, a strict DRM would probably make fair use a nonexistent thing. (Fair use is defined by Calem [1997, p. 1] as “*a doctrine that allows the general public to use some copyrighted materials for certain purposes*”.)

Gilmore (2001) discusses and exemplifies several problems with what he calls copy protection (DRM can be seen as a kind of copy protection): elimination of competition, copy protection can be abused, policies are not created in open discussions, freedom of speech and of the press are threatened, just to name some of them. These problems are indeed real, but they should not be insurmountable if a balance between users' rights and content providers' interests can be found. DRM systems that only take into account the interests of content providers will not be successful; a good DRM system would be a win-win situation from which both parties can benefit, although in different ways.

Bechtold (2003) writes that even though DRM may interfere with fair use and innovation, it can also have positive implications in these areas. DRM is not a single technology but is rather flexible and capable of being used for a whole range of different purposes. It is important to note that DRM systems could be built that take into account fair use and other rights that users are guaranteed through laws.

DRM systems have privacy implications since the purpose is to keep track of users so as to know who is allowed what rights to certain content, and this gives content providers the means for monitoring people's preferences in terms of books, music,

## 7 Discussion

movies, etc. Bechtold (2003) acknowledges these risks, but he also sees a potential for consumers to benefit from this since it would allow better personalization of services. There must be a balance between user privacy and convenience. The benefit of DRM for users from a privacy perspective would be that it allows users to control who can read their personal information and what they can do with it (Bechtold, 2003). DRM systems work both ways.

If a strict DRM system would be developed and implemented in such a way that it would frustrate the majority of users, there is room for a large market of DRM circumvention tools. For this reason, arguments against DRM based on the system's having weak protection against attacks from the owners is not as far-fetched as it might sound. Paradoxically, if DRM systems that are wholeheartedly disliked by users become widespread, DRM circumvention tools would probably flood the market. With such tools easily available to users, the DRM system would actually be quite unreliable for purposes of DRM, and therefore it is not entirely inconceivable that widespread use of a DRM system that can be circumvented (no DRM system is completely secure) would eventually lead to a situation where no one uses it.

DRM system must fully honor users' rights while protecting content from illegal ways of copying, modifying, or using it. If developers of DRM systems do not work with the users, there is a real possibility that the users will strongly oppose such systems, and no one would use them. DRM questions are complex and difficult, but if an appropriate balance can be found between the interests of content providers and consumers, then DRM systems may actually benefit both.

It is the author's conviction that a new approach to computer security and privacy is needed since the computer-based threats are very unlikely to diminish as the computerization of society continues more or less unabated, and trusted computing seems to be a very promising solution. There are risks with trusted computing, but most technological advances suffer from some disadvantage, and at least in this case technology is not the whole story as decisions such as what policies to enforce play a very important role. The author is generally positive to trusted computing and believes that it will eventually be possible to take advantage of its benefits without having to worry about the risks. Furthermore, the author is looking forward to a future with trusted computing with great interest and optimism.

## References

Anderson, Ross (2003). Trusted Computing Frequently Asked Questions. *Ross Anderson's Home Page*. Available at: <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html> [accessed 2004-02-20].

Arbaugh, Bill (2002). Improving the TCPA Specification. *IEEE Computer*, vol. 35, no. 1, pp. 77-79.

Bechtold, S. (2003). The Present and Future of Digital Rights Management: Musings on Emerging Legal Problems. In: *Digital Rights Management: Technological, Economic, Legal and Political Aspects*, E. Becker, W. Buhse, D. Günnewig, & N. Rump (eds.), pp. 597–654, Berlin: Springer. Available at: [http://www.jura.uni-tuebingen.de/bechtold/pub/2003/Future\\_DRM.pdf](http://www.jura.uni-tuebingen.de/bechtold/pub/2003/Future_DRM.pdf) [accessed 2004-02-07].

Calem, R.E. (1997). “Fair Use” and International Treaties. *The New York Times*. Available at: <http://www.nytimes.com/library/cyber/week/052197watermark-side.html> [accessed 2003-03-21].

Carroll, A., M. Juarez, J. Polk, & T. Leininger. (2002). Microsoft “Palladium”: A Business Overview. *Microsoft Corporation Web site*. Available at: <http://www.microsoft.com/presspass/features/2002/jul02/0724palladiumwp.asp> [accessed 2003-02-18].

Cavoukian, A. & D. Tapscott. (1997). *Who Knows: Safeguarding Your Privacy in a Networked World*. McGraw-Hill: New York, USA.

Chapman, D.B. & E.D. Zwicky. (1995). *Building Internet Firewalls*. O'Reilly & Associates: Sebastopol, CA. USA.

DRM is Great, But It Won't Work (2004). *Invisiblog Web site*. Available at: <http://invisiblog.com/1c801df4aee49232/article/85eae13c6151d60fa610cfd2d0f210c> [accessed 2004-05-02].

Dudley, Brier (2003). Microsoft gives up on “Palladium” trademark. *The Seattle Times*. Available at: [http://seattletimes.nwsourc.com/html/business/technology/134621649\\_microsoftpalladium25.html](http://seattletimes.nwsourc.com/html/business/technology/134621649_microsoftpalladium25.html) [accessed 2003-03-15].

EFF Report on Trusted Computing (2003). *Invisiblog Web site*. Available at: <http://invisiblog.com/1c801df4aee49232/article/b8d4198c44af778cc8833ea371011b9> [accessed 2004-03-02].

## References

Gilmore, John (2001). What's Wrong With Copy Protection. *John Gilmore's Web site*. Available at: <http://www.toad.com/gnu/whatswrong.html> [accessed 2003-07-09].

Interesting Uses of Trusted Computing (2004). *Invisiblog Web site*. Available at: <http://invisiblog.com/1c801df4aee49232/article/0df117d5d9b32aea8bc23194ecc270ec> [accessed 2004-03-23].

Interesting Uses of Trusted Computing, Part 2 (2004). *Invisiblog Web site*. Available at: <http://invisiblog.com/1c801df4aee49232/article/6b607597c4c3ad8ca8a72fd4cf5d1b91> [accessed 2004-03-23].

Internet Voting, Safely (2004). *Invisiblog Web site*. Available at: <http://invisiblog.com/1c801df4aee49232/article/9d481af00c898ae91748f2f0cd97cf80> [accessed 2004-03-23].

Lettice, John (2003). Bad publicity, clashes trigger MS Palladium name change. *The Register*. Available at: <http://www.theregister.co.uk/content/4/29039.html> [accessed 2003-03-14].

Loney, Matt (2002). Dissecting Palladium: DRM or not DRM? *ZDNet UK Web site*. Available at: <http://comment.zdnet.co.uk/story/0,,t479-s2118863,00.html> [accessed 2003-02-26].

Microsoft (2002). Q&A: Microsoft Seeks Industry-Wide Collaboration for "Palladium" Initiative. *Microsoft Corporation Web site*. Available at: <http://www.microsoft.com/presspass/features/2002/jul02/07-01palladium.asp> [accessed 2003-12-18].

Microsoft (2003a). Security Model for the Next-Generation Secure Computing Base. *Microsoft Corporation Web site*. Available at: [http://www.microsoft.com/resources/ngscb/documents/NGSCB\\_Security\\_Model.doc](http://www.microsoft.com/resources/ngscb/documents/NGSCB_Security_Model.doc) [accessed 2004-01-09].

Microsoft (2003b). At WinHEC, Microsoft Discusses Details of Next-Generation Secure Computing Base. *Microsoft Corporation Web site*. Available at <http://www.microsoft.com/presspass/features/2003/may03/05-07NGSCB.asp> [accessed 2004-01-09]

Microsoft (2003c). Microsoft Next-Generation Secure Computing Base – Technical FAQ. *Microsoft Corporation Web site*. Available at: <http://www.microsoft.com/technet/security/news/ngscb.msp> [accessed 2004-01-09].

## References

- Orlowski, A. (2001). The Microsoft Secure PC: MS patents a lock-down OS. *The Register*. Available at: <http://www.theregister.co.uk/content/archive/23387.html> [accessed 2003-03-21].
- Pearson, S. (2002). How Can You Trust the Computer in Front of You? *HP Labs Web site*. Available at: [http://www-uk.hpl.hp.com/trust-security-privacy/external/publications/tech\\_reports/HPL-2002-222.pdf](http://www-uk.hpl.hp.com/trust-security-privacy/external/publications/tech_reports/HPL-2002-222.pdf) [accessed 2003-03-15].
- Pfleeger, C. P. (1997). *Security in Computing* (second edition). Prentice-Hall International: Upper Saddle River, NJ, USA.
- Russell, D. & G.T. Gangemi (1991). *Computer Security Basics*. O'Reilly & Associates: Sebastopol, CA, USA.
- Safford, David (2002). Clarifying Misinformation on TCPA. *IBM Research — Global Security Analysis Lab Web site*.  
[http://www.research.ibm.com/gsal/tcpa/tcpa\\_rebuttal.pdf](http://www.research.ibm.com/gsal/tcpa/tcpa_rebuttal.pdf), 2003-07-09
- Schechter, S.E., R.A. Greenstadt & M.D. Smith (2003). Trusted Computing, Peer-To-Peer Distribution, and the Economics of Pirated Entertainment. Presented at *The Second Workshop on Economics and Information Security*, College Park, Maryland, May 29–30, 2003. Available at: <http://www.eecs.harvard.edu/~stuart/papers/eis03.pdf> [accessed 2003-06-24]
- Schoen, S. (2003). Trusted Computing: Promise and Risk. *Electronic Frontier Foundation Web site*. Available at: [http://www.eff.org/Infrastructure/trusted\\_computing/20031001\\_tc.php](http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.php) [accessed 2003-12-13].
- TCG (2003a). New trusted computing group formed to advance the adoption of open standards for trusted computing technologies (press release). *Trusted Computing Group Web site*. Available at: [https://www.trustedcomputinggroup.org/press/news/2003\\_04\\_08\\_tcg\\_formed.pdf](https://www.trustedcomputinggroup.org/press/news/2003_04_08_tcg_formed.pdf) [accessed 2004-01-09].
- TCG (2003b). Trusted Computing Platform Alliance (TCPA): Main Specification version 1.1b. *Trusted Computing Group Web site*. Available at: [https://www.trustedcomputinggroup.org/downloads/Main\\_TCG\\_Architecture\\_v1\\_1b.zip](https://www.trustedcomputinggroup.org/downloads/Main_TCG_Architecture_v1_1b.zip) [accessed 2004-02-17].

## References

TCG (2003c). TPM v1.2 Specification Changes: A summary of changes with respect to the v1.1b TPM Specification. *Trusted Computing Group Web site*. Available at: [https://www.trustedcomputinggroup.org/downloads/TPM\\_1\\_2\\_Changes\\_final.pdf](https://www.trustedcomputinggroup.org/downloads/TPM_1_2_Changes_final.pdf) [accessed 2004-03-16].

TCG (2004a). TCG talks about the recent European Union report on TCG and its specifications. *Trusted Computing Group Web site*. Available at: [https://www.trustedcomputinggroup.org/press/feb\\_6\\_art\\_29\\_report\\_QA.pdf](https://www.trustedcomputinggroup.org/press/feb_6_art_29_report_QA.pdf) [accessed 2004-04-26].

TCG (2004b). Trusted Computing Group: Frequently Asked Questions. *Trusted Computing Group Web site*. Available at: <https://www.trustedcomputinggroup.org/about/faq/> [accessed 2004-03-01].

TCPA (2000). Building A Foundation of Trust in the PC. *Trusted Computing Platform Alliance Web site*. Available at: [http://www.trustedcomputing.org/docs/TCPA\\_first\\_WP.pdf](http://www.trustedcomputing.org/docs/TCPA_first_WP.pdf) [accessed 2003-03-15].

TCPA (2001). TCPA Design Philosophies and Concepts, Version 1.0. *Trusted Computing Platform Alliance Web site*. Available at: [http://www.trustedcomputing.org/docs/designv1\\_0final.pdf](http://www.trustedcomputing.org/docs/designv1_0final.pdf) [accessed 2003-03-15].

TCPA (2002a). Trusted Computing Platform Alliance: A Technical Overview of Trusted Computing. *Trusted Computing Platform Alliance Web site*. Available at: [http://www.trustedcomputing.org/docs/tcpa\\_tech\\_ov.pdf](http://www.trustedcomputing.org/docs/tcpa_tech_ov.pdf) [accessed 2003-02-22].

TCPA (2002b). TCPA Overview (presentation). *Trusted Computing Platform Alliance Web site*. Available at: [http://www.trustedcomputing.org/docs/TCPA\\_Layout\\_%20v1.3.pdf](http://www.trustedcomputing.org/docs/TCPA_Layout_%20v1.3.pdf) [accessed 2003-03-15].

TCPA (2002c). The Evolution of the Trusted PC (brochure). *Trusted Computing Platform Alliance Web site*. Available at: [http://www.trustedcomputing.org/docs/14\\_industry\\_1.pdf](http://www.trustedcomputing.org/docs/14_industry_1.pdf) [accessed 2003-03-15].

TCPA (2002d). TCPA Frequently Asked Questions. *Trusted Computing Platform Alliance Web site*. Available at: [http://www.trustedcomputing.org/docs/Website\\_TCPA%20FAQ\\_0703021.pdf](http://www.trustedcomputing.org/docs/Website_TCPA%20FAQ_0703021.pdf) [accessed 2003-03-20].

TCPA (2002e). TPM Q&A. *Trusted Computing Platform Alliance Web site*. Available at: [http://www.trustedcomputing.org/docs/TPM\\_QA\\_1016021.pdf](http://www.trustedcomputing.org/docs/TPM_QA_1016021.pdf) [accessed 2003-02-20].