"For years, Bill Gate has dreamed of finding a way to make the Chinese pay for software: TC looks like being the answer to his prayer."
– Ross Anderson [Reference 7]

The Trusted Computing (TC) and Next Generation Secured Computing Base (NGSCB)

Version 1.0

Spring 2005

Computer Networking Management

By:

Jianji (Joseph) Yu

Jeffrey Khuu

Table of Contents

1. Introduction

Overview

1.1 The Trusted Computing

✧ Trusted Computing (TC)

The term Trusted Computing (TC) means the computer security integrated with hardware and software security components. As Ross Anderson suggested, the original motivation of TC was intended for digital rights management (DRM); that limits the abuse of file sharing over the network and making illegal copies without the authorization from the vendors, perhaps, restrict user's computing actions. However, current motivations and applications for trusted computing extend way more than DRM: such as giving too many authorizations to the computers over users. The fundamental concept of TC is that the software runs and communicates securely over applications and servers. TC can be referred as a “locked-down” architecture such that it has hardware level cryptographic keys for encryption and authentication. It was also tamper-resistant; seal secure data within curtained memory, and input/output communication path are encrypted. Users have no way to share their file contents; simply, they could not open the files. Each computing action is required to run through the Nexus, the main security core of NGSCB. TC had made several hardware changes to make it tamper resistance, memory security, and encryption keys. Those important keys were stored and sealed within the hardware. Currently, there are many hardware vendors already provide the hardware support for major required components of NGSCB such as Intel provided their LaGrande Technology (LT) and AMD’s Secure Execution Mode (SEM). The term, Trusted Computing Group (TCG) is an alliance of Microsoft; its purpose is to manage the TC activities for Intel, AMD, HP, IBM, and other major computer technology companies.

✧ Trusted Computing Base (TCB)

We often use the term “trusted computing” daily. But what exactly is trusted computing? In order to answer this question, we have to go further and have to understand the meaning of “trusted computing base”. The Trusted Computing Base (TCB) is a part of the system that combines the hardware and software components that were designed to take the responsibility for regulate the information security policies of the computer system. The TCB software consists of the kernel (“operating system”) and configuration file that controls the system operation and “any program that runs with the privilege or access rights to alter the kernel or the configuration files.” [Reference 2] In another words, TCB is everything in operating system that we reply on for security. If TCB is damaged or not-secured, the security of the whole system is broken. However, if everything outside TCB is damaged or not-secured, we still have trusted system. [Reference 1]

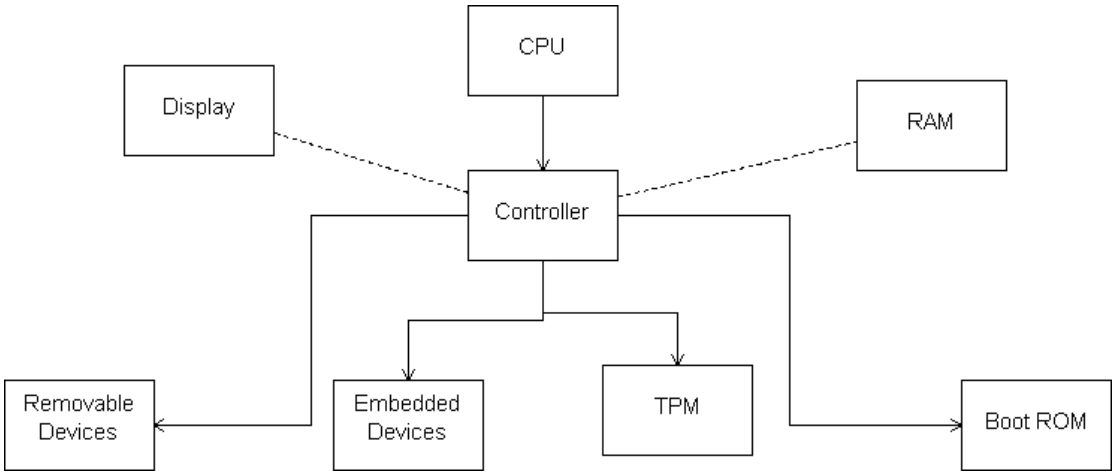
✧ Trusted Computing Group (TCG)

The goal of Trusted Computing Group (TCG) is to provide a secured Trusted Computing Base (TCB) for the system. As we talked about earlier, TCG is a group of hardware vendors that

coordinates the TC activities. The TCG was formed in spring 2003 and adopted the specification which was developed by the Trusted Computing Platform Alliance (TCPA). TCG is also a nonprofit industry standards organization to enhance the security of computing environment by collaborates with different platforms, software, and technology vendors. To sum up, TCG wants to provide a secure hardware and software operating system that enhances computer user's trusted domains. The TCG publicly published industry specification standards such as architectures, function methods, and interfaces. So the vendors could follow the guidelines for a wide variety of computing platform designs, implementations and validations. Platforms based on TCG specifications are expected to delivery secure and reliability standards for all computing needs.

♦ TCG Architecture

The following is a TCG reference architecture model for personal computers and PDAs. [Reference 3]



♦ Features

A trusted platform has served three basic features: protected capabilities, integrity capabilities, and integrity reporting. These three basic fundamental features should provide a trusted platform where we expected the computing behave the way we wanted and "do what we wanted securely". [See reference 5]

1.2 Next Generation Secured Computing Base (NGSCB)

Microsoft is one of main followers for Trusted Computing. They called their version of TC as the Next Generation Secured Computing Base (NGSCB). Basically the NGSCB can be described as two modes, normal mode and trusted mode. The normal mode will work very much same as our current Windows, fully controlled by the user. However, the trusted mode will be using locked-down architecture, where the computer is controlled by the computer not the users. Users have no authorities to perform modify, delete, and copy operations. All the operations are controlled by the nexus. This feature has raised many issues such as freedom of computing, personal rights, and other moral issues.

2. NGSCB

2.1 Features

2.1.1 The two operating environments

As we discussed earlier, NGSCB operates two operating systems within one system. In this section, we are going to discuss more detail this NGSCB system in Microsoft's term. According to Microsoft, there are two operating systems that reside in NGSCB. One is operating non-secure processes. Another one is operating secure processes. Microsoft referred the non-secure operating system as left-hand-sided system where the secure operating system as right-hand-sided system. The nexus computing agent (NCA) is the agent who communicates between two isolated operating systems. Microsoft claimed that “only an NGSCB trusted application, NCA, can run securely within the protected operating environment.” (Reference 5) The NCA can be defined specific regarding its policies about the software by the software developers such as setting the security authentication and authorization of the software. [See reference 8]

2.1.2 Four Features of NGSCB

There are four core elements of security features that provide through the NGSCB. The four features are the following: Strong process isolation, Sealed storage, Attestation, and Secure paths to the user. Each features served its role to provide user better security in computing. Without one of the features, the NGSCB will not be secured anymore. As Microsoft described that “the goal of integrate all these features is to provide user a secure platform” and not disturbed user’s regular computing. [See reference 8, 9]

✧ Strong process isolation

This feature is to isolate the protected and non-protected operating environment that exists in the memory allocations. Since the protected and non-protected operating environments are stored in the same memory environment, it’s an important requirement to restrict and protect address space for those applications that resides in protected operating environment. NGSCB addresses this requirement by isolate a specific portion of Random Access Memory (RAM) within the address that entitled to the secure area where the non-secure application cannot be accessed. In addition, NGSCB blocks the access of Direct Memory Access (DMA) devices in term of writing and reading to secured block of memory. It aims to block access of malicious code that trying to read or write to the secured block of memory. [See reference 5] With strong process isolation feature, no unlegimate access will be occurring in protected environment.

✧ Sealed storage

This feature is another term for file access control in operating system which aims to ensure the privacy of NGSCB data that not being exposed. NGSCB implemented the so-called Security Support Component (SSC) to ensure the security of sealed data storage. The SSC has its own encryption services and it can be managed by the core of protected environment, the nexus. The services including pair of public and private key and the keys derived for

trusted application and service by using Advanced Encryption Standard (AES). An NCA uses these keys to encrypt data, access file system, and provide the storage services. Microsoft claimed that the “Protected information is accessible only to the software that stored it and can only be accessed when the original SSC is present. “ [Reference 6] That means that no unauthorized application can read the sealed storage rather it’s from boot up moved to another computer and so on. It’s totally secured. [Also see reference 5]

✧ Cryptographic Attestation

This feature is to confirm that the recipient that the data was digital signed by the NGSCB and the data was cryptographically identifiable. It’s the process that authenticates the software; prove its identity, before any data are being processed. This feature came in very useful for those networked application where prove its identity securely before transmit any data. It helps to identify that the application that you processing is really the application itself, not mal-wares. For more information about attestation protocol, see reference [6] for more details.

✧ Secure paths to the user

This feature is to ensure the information remains securely through the input and output of the devices. The aim of this feature is to encrypt the input and output so that the system creates a secure path from input devices to trusted application. In another words, this guarantees the transmission of the data along the input/output is secured. It helps to protect the computer from being keystroke recorded, by applying this secure path concept, no program is able to record anything from input devices. According to Microsoft, in order to achieve this goal, users have to use upgraded keyboards and USB devices, which enable the local user to communicate securely with a trusted application. [Reference 5] USB devices are including smart cards, biometrics, and others. For the output portion, some special output devices are needed because most graphic adapters are not concerned of security such that enables software to read or write to video memory. [See reference 5]

2.2Architecture

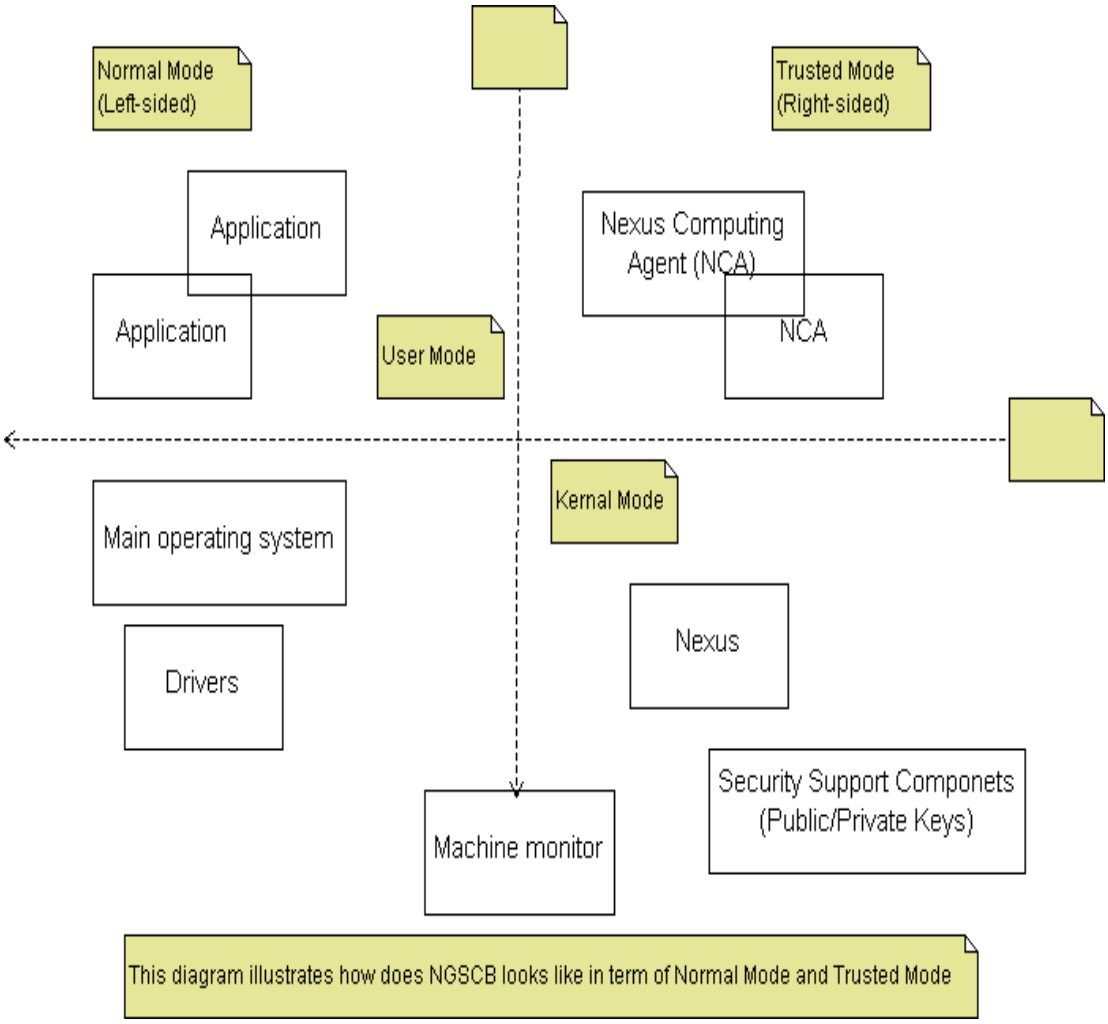
2.2.1 Two primary system components in trusted operating environment

- **Nexus**

  Nexus is referring a special security kernel that act as the core of the trusted operating environment. The purpose of Nexus is to isolate the process of normal mode and trusted mode differently in the memory. Its functionality includes the following: authenticate and protect data (entered, stored, communicated, and displayed) by providing data encryption

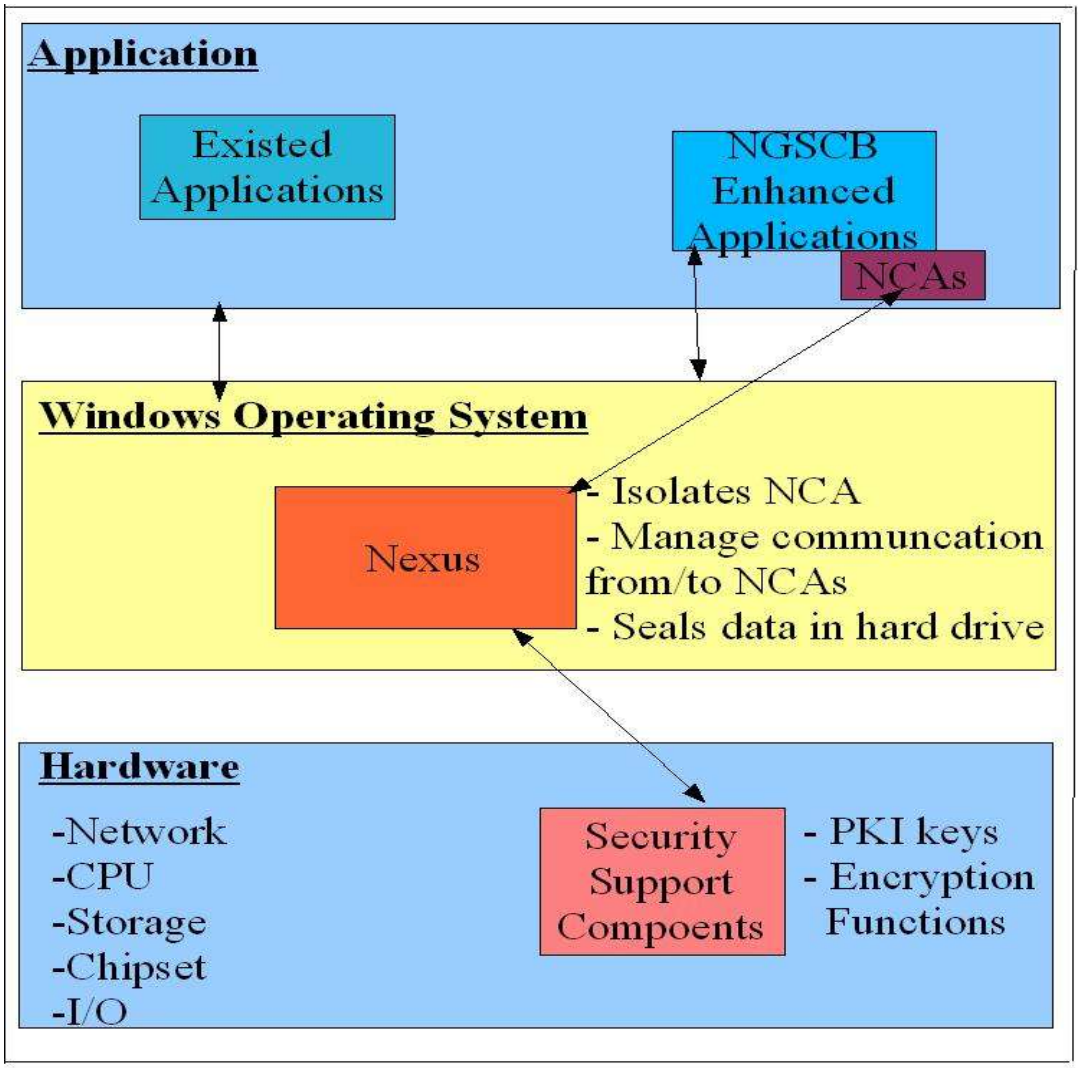
- **Nexus Computing Agent (NCA)**

  An NCA is the trusted software component that can be a part of the program, application, or service, which runs in the trusted mode that communicates with the Nexus. Microsoft has also published the source code for NCA so that software developers can make their own agent to run on trusted platform.


Normal Mode
(Left-sided)
Trusted Mode
(Right-sided)
Application
Application
Nexus Computing
Agent (NCA)
NCA
User Mode
Kernal Mode
Main operating system
Drivers
Nexus
Security Support Componets
(Public/Private Keys)
Machine monitor
This diagram illustrates how does NGSCB looks like in term of Normal Mode and Trusted Mode

2.3 NGSCB Summary

As we have discussed so far, the primary goal of NGSCB was to design a secured and trusted platform. The protected and trusted operating environment is physically isolated memory from the system itself. The block of trusted memory is resistant to malicious codes, mal-wares, and other attacks. The secure path feature making the trusted code cannot be recorded and modified within trusted mode environment. As a summary, the following figure shows how do NGSCB helps to protect users and provide them a very secure platform of computing.



This diagram shows the interaction between applications, operating systems, and hardware device

3. Analysis of NGSCB

3.1 The current problematic computing

Currently, user can do whatever they wanted to do in computer. In another words, current user is taking the responsibility to control the computer such as read, modify, and delete operations to the stored on their hard drives. As a networking perspective, user can take control of the computer such as modify the firewall settings and do whatever they wanted to interacted with the world. Perhaps, user can share his or her files to others by using peer-to-peer protocol programs or easily distributed them over the internet. The problems challenged this kind computing such that user can be infected keystroke record wares, virus, worms, and spy-wares very easily. The worms' installation to the computer might go under behind the user's awareness and so on. That's a need for NGSCB, which protected the user from being attacked or installed mal-wares. However, there are many criticized about NGSCB though. It started to raise the issues about ownership, censorship, and computing freedom. Users do not like to be controlled in many ways. It is also questionable that rather the ownership of the PC because NGSCB gives the authorization ("power") to the program/application creator who can control over the users such as restrict their access the program, prevent they make any copies.

3.2 Application

There are many applications that involved NGSCB, including regular computing and networking aspects. For regular computing, the enhanced NGSCB version of Microsoft Word will put the restriction to the user whether they have the rights to view the content of the document or rights to copy and paste from current document to another document. With NGSCB technology, users will not able to open the document with another application, say OpenOffice. The document is signed and encrypted in Microsoft Word; it meant that only Microsoft Word has the private key to decrypt it. The same problem also exists in networking application, suppose you want to check your email via Microsoft's Outlook. You might be able to view your email content but you might not have the rights to copy and paste your email.

3.3 Will NGSCB be the solution?

It's human nature to take control over things and not controlled by others. The NGSCB is developed way too forced and restricted user's authentication and authorization of computing. People will not use it if it blocks and restricts them doing what they want to do. The more Microsoft and TCG push NGSCB, the sooner people will leave Microsoft product and use other alternatives such as Apple OS or Linux. It's like Anderson suggested the motivation behind Microsoft is to make people to pay for their software. However, that won't work. Companies will not tolerate attestations on the network and through the firewall every time their employee wants to open a file. It's really troublesome. Perhaps, NGSCB will fail to work for DRM because there is always ways to workaround of things. For example, the operating system is trying to restrict people to make copies of music such that the pathway is encrypted all way to the speakers; user can still record what comes out the speaker and creates the MP3 out of it. In addition, if user wants to copy and paste their document, they can take the digital photograph of their screen and owns the copy of it. As a summary of our paper, we concluded that NGSCB and the Trusted Computing will not work in the future.

References

[1] Mark Stamp's CS166 software presentation slides
http://www.cs.sjsu.edu/~stamp/CS166
[2] System Management Concepts: Operating system and Devices
http://www.unet.univie.ac.at/aix/aixbman/admnconc/tcb.htm
[3] TCG Specification Architecture Overview
https://www.trustedcomputinggroup.org/downloads/TCG_PCSpecificSpecification_v1_1.pdf
[4] Microsoft's Next Generation Secured Computing Base Overview
http://www.microsoft.com/resources/ngscb/NGSCB_Overview.mspx
[5] NGSCB Security Model
http://www.microsoft.com/resources/ngscb/documents/NGSCB_Security_Model.doc
[6] Trusted Computing and NGSCB
http://www.cs.bham.ac.uk/~mdr/teaching/TrustedComputing.html
[7] Ross Anderson's Trusted Computing FAQ
http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html
[8] Microsoft's resource for NGSCB
http://www.microsoft.com/resources/ngscb/productInfo.mspx
[9] Microsoft's NGSCB four features
http://www.microsoft.com/resources/ngscb/four_features.mspx