ISSN 0974 - 9373

Vol. 15(2011) Special Issue 2 **Journal of International Academy of Physical Sciences** pp. 445-453

Next-Generation Secure Computing Base (NGSCB)*

Krishan Kant Lavania, Mohit Gupta and Nitish Jain
Department of Information Technology
Arya Institute of Engineering & Technology, Jaipur, Rajasthan, India
Email: k@lavania.in; mohitpalash@gmail.com; nitishjaincool@gmail.com

Surendra Sharma
Department of Computer Engineering
Arya Institute of Engineering & Technology, Jaipur, Rajasthan, India

(Received June 14, 2011)

Abstract: In June 2002, Microsoft released information regarding its new initiative named as "Palladium". Palladium is a system which combines hardware and software controls to create a "trusted" computing platform. In doing so, Palladium would establish an unprecedented level of control over users and their computers. It could place Microsoft as the gatekeeper of authentication and identification. Apart from this, it is also provide systems embedded in both software and hardware would control access to content, thereby creating ubiquitous Digital Rights Management schemes that can track users and control use of media. Microsoft believes to have elements of this system in place in the year 2004. Later, Microsoft called it NEXT-GENERATION SECURE COMPUTING BASE. Here Microsoft is try building a trustworthy computing environment to help customers realize their full potential. From the start of this initiative, Microsoft's vision has been to create new security technology for the Microsoft Windows platform that uses a unique hardware and software design to give people new kinds of security and privacy protections in an interconnected world[1]. The vision of Microsoft has not changed. Their original approach was to create a new secure computing base that would run parallel to the regular environment of windows. This environment would provide features such as sealed storage, strong process isolation, secure path to and from the user and attestation. This approach would have required that the applications be rewritten to take advantage of the new secure computing base.

In this paper we will be discussing the design goals and implementation of 'NGSCB'. Later we will see the advantages and criticism of it.

Keywords: Palladium, NGSCB, Trusted Computing, Attestation, Digital Rights Management (DRM), Trusted Service Provider (TSP), Trusted Platform Module (TPM).

*Paper presented in CONIAPS XIII at UPES, Dehradun during June 14-16, 2011.

1. Introduction

The Next-Generation Secure Computing Base (NGSCB) which formerly known as Palladium, is a software architecture designed by Microsoft which is expected to implement "Trusted Computing" concept on future versions of the Microsoft Windows operating system[2]. Palladium is part of Microsoft's Trusted Computing initiative. Microsoft's stated aim for palladium is to increase the security and privacy of computer users. Palladium involves a new breed of hardware and applications in along with the architecture of the Windows operating system. Designed to work side-by-side with the current functionality of Windows, this significant evolution of the personal computer platform will introduce a level of security that meets the rising customer requirements for data protection, integrity and distributed collaboration. It's designed to give people greater security, personal privacy and system integrity. Internet security is also provided by palladium such as protecting data from virus and hacking of data.

In addition to new core components in Windows that will move the Palladium effort forward, Microsoft is working with hardware partners to build Palladium components and features into their products. The new hardware architecture involves changes to CPUs which are significant from a functional perspective. There will also be a new piece of hardware called for by Palladium that you might refer to as a security chip. It will provide a set of keys and cryptographic functions that are central to what we're doing. There are also some associated changes under the chipset, and the graphics and I/O system through the USB port—all designed to create a comprehensive security environment.

"Palladium" is the code name for an evolutionary set of features for the Microsoft Windows operating system. When combined with a new breed of hardware and applications, "Palladium" gives individuals and groups of user’s greater data security, personal privacy and system integrity. Designed to work side-by-side with the existing functionality of Windows, this significant evolution of the personal computer platform will introduce a level of security that meets the rising customer requirements for data protection, integrity and distributed collaboration.

2. Design Goals-The Four Fundamentals

A. Strong Process Isolation

The protected operating environment isolates a secure area of memory which is used to process data with higher security requirements. Windows currently provides separation by using ring 3 and ring 0 processor mode isolation. Windows and any other operating systems also make use of virtual memory segmentation to separate processes from the operating system and from each other. Virtual memory which is used to be considered hard process isolation but Microsoft makes a remarkable admission that "Using the current memory scheme, only virtual memory protection is achievable, and it is relatively easy for an attacker to add malicious programs to both the operating system and user space memory". An interesting thought is to explore here is that under NGSCB even if Windows is completely compromised, the NGSCB components can still provide privacy and integrity.

B. Sealed Storage

This storage method uses encryption to help ensure the privacy of NGSCB data that persists on the hard disk of NGSCB-capable computers. Sealed storage is secure information storage on the hard disk. Sealed storage is provided through the use of a security support component (SSC) which is implemented directly in hardware. This feature provides the notion of a long-lived confidential binding between an application and its data. A primary threat addressed is that even if any another operating system is booted or if any hard drive is moved to another computer the data should stay confidential.

C. Attestation

This occurs when a code digitally signs and attests to a piece of data which help to confirm to the recipient that the data was constructed by a cryptographically identifiable software stack. This idea is different and new. Attestation allows an application to both identify a remote partner application and satisfy a requirement that the remote application has integrity. This integrity is provided by a "cryptographically identifiable software stack". Microsoft introduces the idea of an application private network (APN). Considering an OSI model and current VPN mechanisms, such as IPSEC, protect data up through layer 4. With an APN data is protected layer 7 to layer 7.An analogue is receiving a phone call from a trusted and an old friend. If you believe that your phone is not tapped and you recognize the patterns, mannerism, and intonations of the voice at the

other end then you may be assured that your conversation is private and that you are indeed just speaking to your old friend.

D. Secure Paths to the User

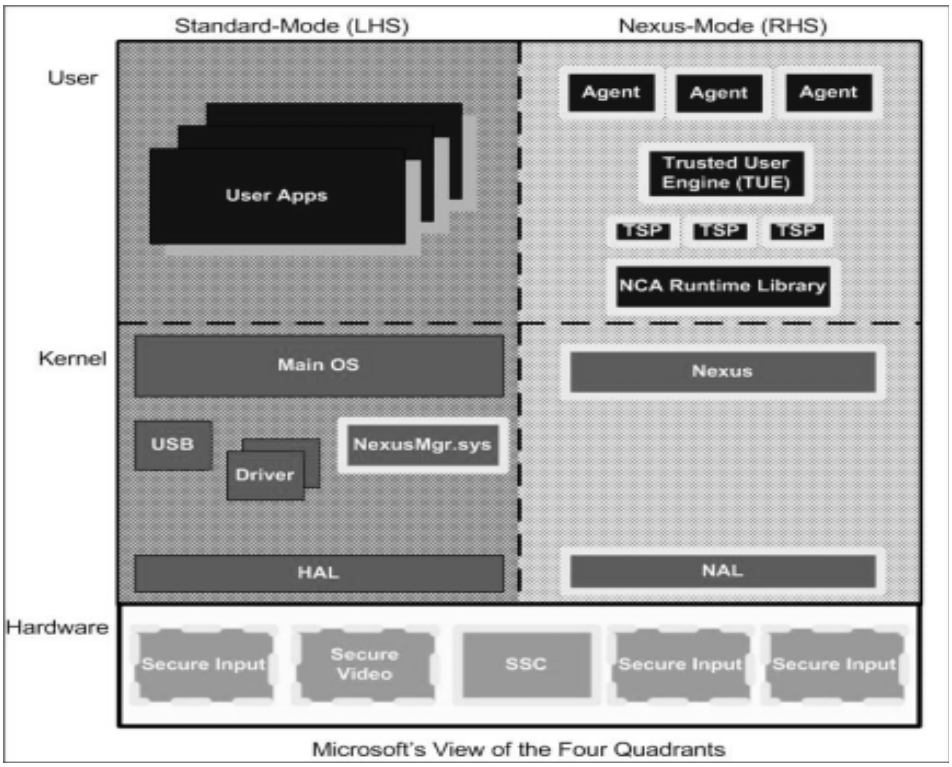
By encrypting I/O, the system creates a secure path from the mouse and keyboard to trusted applications and from those applications to a region of the computer screen. These secure paths ensure that valuable information remains unaltered and private. Interestingly this is not a new idea, but this idea has never been widely implemented in a general purpose computer/OS environment. Secure path specifically means that keyboard input is protected from key press until consumed by a secure mode application (other input devices such as smart card readers and biometric units may be added later). The secure paths also means provides a mechanism to denote which area(s) of the screen are secure and secure output—secure output being a modified graphics adapter—where the adapter card protects against screen scraping. Microsoft emphasizes the difference between the terms secure path and secure channel. Means secure path is a protected path between the computer and the user and secure channel is a protected channel between two computer applications.

3. Design Implementation– Living in a Bi-Polar World

The Left Hand Side (LHS) represents the PC hardware and architecture as we know it. The LHS represents the future computing model too for non-NGSCB enabled OS's. There's NO any change if NGSCB is not enabled. The Right Hand Side (RHS) is the part where all the new security features are implemented. If NGSCB is widely adopted then the LHS will immediately connote insecure and RHS will connote secure. If the NGSCB services are required then there is an addition of a device driver, the NexusMgr.sys, on LHS. It is responsible for loading the Nexus, and for calling the Nexus for NGSCB services. The NexusMgr provides service and coordination also for Nexus and RHS applications. The services, NexusMgr provides for the RHS are: device driver (I/O), file system, memory management, windows management coordination, and user debugging.

Support of RHS requires some hardware changes. The CPU should support a mode flag and context switching between LHS & RHS. The CPU must ensure that memory that is marked as trusted can be accessed by the RHS. CPU must support nexus initialization. Overall NGSCB chipset must prevent bus mastering devices, including DMA, from accessing memory. The NGSCB motherboard must contain a SSC (System Security Component). This device is also known as TPM—Trusted Platform Module. The SSC also provides functions such as RSA public key operations, AES

encryption and decryption, and SHA-1 hash computation. The SSC stores at least one RSA private key and one AES key.



The new architecture of Intel is to support NGSCB is called Le Grande after a town in Oregon (as Intel says they are developing Le Grande to support secure computing, and it would be nice if SW companies would make the small changes needed to support it). The AMD initiative, for now, is call Secure Execution Mode (SEM) and is "2 or 3 years away". As mentioned earlier, keyboards and graphics cards must be modified to encrypt data from key press until display upon the video screen to support secure paths. The security kernel, a mini-operating system that runs in the RHS, is known as the nexus. The nexus is supposed to be sized between 100K to 300K lines of code to foster review and provability. This sounds reasonable to me. At one time it was an expert on IBM's Virtual Machine (VM) operating system. The Control Program (CP-which had little user interface, no file system, etc.) of that OS at one time was about 300K lines. I found 300K lines to be understandable and knowable—but not sure how much higher this number

can go while maintaining intuitiveness. The nexus contains no device drivers. The Nexus does not support any file system. All file operations and input/output must be passed to the LHS. The nexus does include services such as process, memory, and thread management. Paging is not supported in the RHS. The nexus is interruptible. When interrupted the nexus must save state and pass the interrupt back to the LHS where the NexusMgr will replay it. To support multiple CPU and SSC-TPM vendors there is a NAL—Nexus Abstraction Layer, similar to the Hardware Abstraction Layer (HAL). The user will choose which nexus to run. But the nexus will be unconditionally trusted. "Because of the importance of nexus source code, it will be made available for inspection, and so will the procedures designed to assure that the hash of the nexus can be verified against the source code producing it."The Windows OS kernel (LHS) will require less than 200 lines of code to support NGSCB[3]. The NexusMgr provides required services for both RHS and LHS—again the NexusMgr, and all LHS services, are not trusted. The idea is that the LHS has the unmitigated power for a DOS. However the LHS will not be able to affect the confidentially and integrity of the RHS. The nexus will be able to be loaded and unloaded at any time without affecting the stability of the Windows OS. The LHS will cause the nexus to be loaded. Several new hardware instructions are required. Most importantly there is a function for the hardware to perform an atomic cryptographic hash of the nexus image. The applications of RHS are known as Nexus Computing Agents (NCAs). Only "good" applications should be allowed to run in the RHS. Instead of just directly using a hash of a program an XML document known as a *manifest* will represent an NCA. The manifest may directly include a hash of the program or may allow the program to be identified by a public key. The manifest identifies modules to be loaded as a part of the NCA, supplies names to be associated with the NCA, and provides version numbers. The manifest also includes a debug flag—meaning that the NCA supports a debugger. I don't have an understanding of how (or even if) secure debugging could possibly happen. The Trusted User Interface engine (TUE) supports a set of XML based dialogue management; it was also called a mini-MFC (Microsoft Foundation Class). The Trusted Service Providers (TSPs) provide common library function.

4. Advantages of NGCB

NGSCB and Trusted Computing is meant as an implementation of Trusted Computing, its potential uses are therefore similar. Proponents claim that Trusted Computing will make computers safer, less prone to viruses and malware, and thus more reliable from an end-user perspective. In addition, they claim that Trusted Computing will allow computers and servers to offer improved computer security over that which is currently available.

A. Digital Rights Management

By utilizing the curtained memory, attestation and cryptographic features of the TPM, a secure form of Digital Rights Management (DRM) may be developed; critics charge that although it does not provide DRM features itself, DRM is nevertheless the primary motivation for the development of NGSCB. DRM would be implemented by encrypting DRM-protected files and making the decryption key available to corporate trusted applications only. A wide range of copy-protection and similar features could be implemented, limited only by the imagination. E.g. it would be possible to create a file which can only be read on one computer, or within one organization, or a file that can only be opened for reading three times. While any DRM-protected file could be just as easily read or copied as an unprotected file, it would be extremely difficult to decrypt the file at an unauthorized destination, rendering it useless.

B. Network Access

In educational and corporate networking environments, a desirable feature of NGSCB is the ability of each workstation to securely attest that no unauthorized modifications have been made either to its hardware or software. A workstation which is unable to authenticate itself can then be automatically denied access to some or all network services at will[4].

C. Owner Override

Critics have proposed 'Owner Override' is a potential solution to these problems. In such a system, the stored key by the TPM would still be inaccessible. But, a secure method is provided to the owner to identify them would be provided, and by this method the owner would be able to force the TPM to make a false attestation or decrypt data for an application that would not otherwise be allowed access to that data. Due to this feature, owners continue to have ultimate control over their computers and software and data stored on them, although it would also make Trusted Computing useless for purposes such as DRM. Trusted Computing and NGSCB would still have some uses in preventing misuse by anyone other than the owner, for example

in a business or educational environment where computing facilities are made available by an school or employer for use by an employee or student.

5. Manageability and Upgrades

There are several activities involving an upgrade that affect the manageability of the NGSCB infrastructure. The key design is to make common manageability tasks simple and safe. The security primitives (like TPM-Unseal and TPM-seal) tightly control the scope of the upgrade. This is important to allowing the widest possible range of use. However, by choosing the default upgrade policy, the upgrade experience can be kept simple and manageable without sacrificing security. Here are the some common upgrade scenarios, in which information about how they are implemented:

A. User upgrades the nexus. How are NCA secrets upgraded?

An upgraded nexus is accompanied by a certificate, which authorizes an existing nexus to seal its secrets to the new nexus. Each generation of a nexus generate a new AES key to save new secrets (gatekeeper key)[5]. This new generated key could protect the existing gatekeeper key. The result is a key hierarchy which allows secrets to migrate to a new version of the nexus as a block (with authorization) while declining, by default, to migrate keys backward from the newer version to the existing version.

B. User upgrades a program. How are NCA secrets upgraded?

The upgraded version of an NCA uses the same manifest as the existing one, so the upgraded version of the NCA gets the same secrets available to the existing NCA. If the NCA authors decide to issue a new manifest, it can, as the nexus does, issue a security credential signed by the same key that signed the original manifest, instructing the existing NCA to seal its secrets to the new version of the NCA.

C. User buys a new computer. How are secrets migrated from one computer to another ?

The Nexus-Seal identity takes an additional argument which indicates to the nexus whether secrets can be unconditionally migrated. When the user buys a new computer, that user logs into the old computer's nexus-side administration user interface, and perform user authentication (for example, by typing a password), and instructs the nexus on the old computer to encrypt its secrets to a public key appearing in a certificate signed by the new nexus. Then the new nexus decrypts the secrets and reseals them under the new nexus-platform AES key. Now the secrets which cannot be migrated unconditionally can be migrated using a protocol either between the NCA on

the old computer and the NCA on the new computer, or among the NCA on the old computer, a trusted server, and the NCA on the new computer.

6. Criticism

Trusted Computing and NGSCB can be used to intentionally and arbitrarily lock certain users out from use of certain files, products and services, for example to lock out users of a competing product, potentially leading to severe vendor lock-in. This is analogous to a problem in which many businesses feel compelled to purchase and use Microsoft Word in order to be compatible with associates who use that software[6]. But today this particular problem is partially solved by products such as OpenOffice.org which provide minimum compatibility with Microsoft Office file formats. Now under NGSCB, if Microsoft Word were going to encrypt documents it produced, then no other application would be able to decrypt them, unless of its ability to read the underlying file format. Trusted Computing and NGSCB are ineffectual at solving the majority of contemporary security problems, for example computer Viruses and Trojans. Despite this, still Microsoft has in the past claimed that NGSCB was necessary to combat the threat of future virus outbreaks against Microsoft Windows users. Microsoft is no longer making claims that NGSCB and Trusted Computing will solve these virus problems.

7. Conclusion

NGSCB and Trusted Computing provide a protected run environment for programs, which isolates them from other programs. Each program is protected from attack (software), even from the operating system. Unlike other authentication models, it is rooted in software authentication and provides software isolation, secure storage, attestation, and secure I/O operations. These features of NGSCB enable the construction of a scalable authentication and authorization security model based on security credentials that allow a broad spectrum of programs to run.

References

1. “Security Model for the NGSCB” Microsoft Paper.
2. NGSCB Homepage.
3. Ross Anderson’s personal website.
4. Trusted Computing.
5. Report on Next Generation Secure Computing Base.
6. www.nextgenerationsecurecomputingbase/wikipedia.html