

Operating System Security: Microsoft Palladium

for
Dr. Chris Taylor
Operating Systems Instructor
Milwaukee School of Engineering
Milwaukee, Wisconsin

by
Karl Heins
CS-384-004

February 3, 2003

TABLE OF CONTENTS

| | |
|--|----|
| ABSTRACT | 1 |
| INTRODUCTION..... | 1 |
| Current Security Problems..... | 1 |
| History | 2 |
| Trusted Computing..... | 2 |
| Trusted Computing Platform Alliance..... | 3 |
| Overview of Palladium Architecture | 4 |
| Definition | 4 |
| Curtained Memory..... | 4 |
| Sealed Storage | 5 |
| Secure Input And Output..... | 5 |
| CORE PRINCIPLES OF PALLADIUM | 5 |
| Hardware | 5 |
| Trusted Space..... | 5 |
| Sealed Storage | 6 |
| Attestation | 6 |
| Software | 6 |
| Nexus..... | 6 |
| Trusted Agents..... | 7 |
| COMPONENTS OF A PALLADIUM SYSTEM | 8 |
| Security Coprocessor | 9 |
| Vaults..... | 11 |
| Nexus | 12 |
| ADVANTAGES OF PALLADIUM | 12 |
| Block Malicious Code | 12 |
| Digital Rights Management..... | 13 |
| DISADVANTAGES OF PALLADIUM..... | 14 |
| Upgrades | 14 |
| Interoperability | 14 |
| Legacy Programs..... | 15 |
| CONCLUSION | 15 |
| BIBLIOGRAPHY | 17 |

ABSTRACT

Arising out of the need for more security and control over the privacy of personal information, Microsoft is developing Palladium, a security technology that is being incorporated into its next operating system. Palladium represents a fundamental change in the way computer software operates. It provides a mechanism, slightly different from the trusted computing initiative developed by the Trusted Computing Platform Alliance, to protect software and data from other software. It will require both new hardware and software to support its promised functionality. Some of its advantages include: blocking malicious code and digital rights management.

Some of its disadvantages include: necessary upgrades, decreased interoperability, and some missing legacy support.

INTRODUCTION

Current Security Problems

More and more, computers are becoming ubiquitous in today's society. We use our computers for work and entertainment. In the process of modern-day computing, a great deal of personal information is accumulated, processed, and exchanged. This has become especially true with the advent of the Internet.

Whether sending an email, making a purchase online, or just surfing a web page, today's computer user is subject to many privacy and security concerns. So it is with these concerns in mind that software developers have decided to improve the reliability and trustworthiness of the modern computing environment. Microsoft

Corporation is one such company that is at the forefront of the so-called “Trusted Computing” initiative. Their stated goal, in accordance with other industry leaders, is to (Carroll A., et al):

- Build solutions that will meet the pressing need for reliability and integrity
- Make improvements to the personal computer such that it can more fully reach its potential and enable a wider range of opportunities
- Give customers and content providers a new level of confidence in the computer experience
- Continue to support backward compatibility with existing software and user knowledge that exists with Windows systems today

The implementation of these ideas has taken the form in Microsoft’s “next-generation secure computing base for Windows” (Carroll A., et al). This undertaking was re-christened as of January 25, 2003. Its former name, Palladium, will be used throughout the remainder of this document for conciseness.

History

In order to understand Microsoft’s implementation of the trusted computing initiative, it is necessary to be aware of what trusted computing means and how it came into existence.

Trusted Computing

Trusted computing, roughly, is a reference to a network of trusted platforms. A Trusted Platform is a platform that can be trusted by local users and by remote

entities. In this context, an entity can be trusted if it always behaves in the expected manner for the intended purpose. The basis for trusting a platform is a declaration by a known authority that a platform with a given identity can be trusted to measure and report the way it is operating. That operating information can be associated with data stored on the platform, to prevent the release of that data if the platform is not operating as expected. Other authorities provide confirmations that describe the operating information the platform ought to produce when it is operating properly. The local user and remote entities trust the judgment of the authorities; so, when they receive proof of the identity of the platform, information about the current platform environment, and proof about the expected platform environment, they can decide whether to trust the platform to behave in a trustworthy and predictable manner (TCPA Design Philosophies).

Trusted Computing Platform Alliance

The Trusted Computing Platform Alliance (TCPA) is an industry work group comprised of over 170 businesses. The TCPA is steered by four member businesses: Compaq/Hewlett Packard, IBM, Intel, and Microsoft (TCPA FAQ). The major deliverable of this organization is a trusted computing specification that will guide industry development of such platforms. With that deliverable, they hope to improve the authenticity, integrity, and privacy of Internet-based communications and commerce (TCPA FAQ). In a noteworthy divergence from the specification laid out by the TCPA, Microsoft is currently developing Palladium, its own specification of trusted computing. It is not clear how much Palladium shares with the TCPA specification. Since the TCPA specification was co-

authored in part by Microsoft, and the Palladium specification is not available, *this report will focus on what is known about the Palladium as it applies to the known TCPA specification.*

Overview of Palladium Architecture

Definition

Palladium is the code name for a set of features for the next Microsoft Windows operating system. Palladium itself is not an operating system. Rather, it is based on architectural enhancements to the Windows kernel and to computer hardware, including the central processing unit, peripherals and chipsets, to create a new trusted execution subsystem (Carroll A., et al). According to Microsoft, Palladium will not break legacy support for the user applications that run on Windows today. While legacy support for today's Windows programs will be supported, they will not benefit from any of the new features Palladium is supposed to offer. New programs will have to be adapted to support Palladium features. Palladium authenticates software and hardware, not users (Carroll A., et al). This is the fundamental idea behind the new technology.

Curtained Memory

Curtained memory refers to the ability of the operating system to hide pages of main memory so that each Palladium application can be assured that it is not modified or observed by any other application (MS Palladium Technical FAQ).

Sealed Storage

Microsoft defines this as the ability to securely store information so that a Palladium application or module can mandate that the information be accessible only to itself or to a set of other trusted components that can be identified in a cryptographically secure manner (MS Palladium Technical FAQ).

Secure Input And Output

According to Microsoft, there will exist a secure path from the keyboard and mouse to Palladium applications, and a secure path from Palladium applications, through the video hardware to a region of the screen. Secure input is intended to prevent keystroke logging and data modification. Secure output is intended to prevent someone from altering the screen in such a way as to trick the user into doing or not doing something (Levy).

CORE PRINCIPLES OF PALLADIUM

Hardware

Trusted Space

Microsoft states that the execution space is protected from external software attacks such as a virus (Carroll A., et al). Trusted space is set up and maintained by the Nexus and has access to various services provided by Palladium, such as sealed storage (Carroll A., et al).

Sealed Storage

According to Microsoft, sealed storage in Palladium means an authenticated mechanism that allows a program to store secrets that cannot be retrieved by non-trusted programs such as a virus or Trojan horse (Carroll A., et al). They also state that other non-trusted programs cannot read information in sealed storage. (Sealed storage can not be read by unauthorized secure programs, for that matter, and cannot be read even if another operating system is booted or the disk is carried to another machine) (Carroll A., et al). These stored secrets can be tied to the machine, the Nexus, or the application. Microsoft states it will also provide mechanisms for the safe and controlled backup and migration of secrets to other machines (Carroll A., et al).

Attestation

By Microsoft's definition, attestation is a mechanism that allows the user to reveal selected characteristics of the operating environment to external requestors (Carroll A., et al). For example, attestation can be used to verify that the computer is running a valid version of Palladium (Carroll A., et al).

Software

Nexus

Microsoft defines the Nexus as the component in Microsoft Windows that manages trust functionality for Palladium user-mode processes (Carroll A., et al). See Figure 1. Also, It provides basic services to trusted agents, such as the

establishment of the process mechanisms for communicating with trusted agents and other applications, and special trust services such as attestation of requests and the sealing and unsealing of secrets (Carroll A., et al). A Nexus, also called a "nub" or "Trusted Operating Root," is essentially the kernel of the Palladium-isolated software stack (MS Palladium Technical FAQ). The Nexus boots the Palladium hardware with a miniature operating system kernel and initializes Palladium services. The Nexus provides a limited set of APIs and services for Palladium applications, including sealed storage and attestation functions (Carroll A., et al).

Trusted Agents

Microsoft states that a trusted agent is a program, a part of a program, or a service that runs in user mode in the trusted space (Carroll A., et al). A trusted agent calls the Nexus for security-related services and critical general services such as memory management. A trusted agent is able to store secrets using sealed storage and authenticates itself using the attestation services of the Nexus (Carroll A., et al). One of the main principles of trusted agents is that they can be trusted or not trusted by multiple entities, such as the user, an IT department, a merchant or a vendor. Each trusted agent or entity controls its own sphere of trust, and they need not trust or rely on each other (Carroll A., et al).

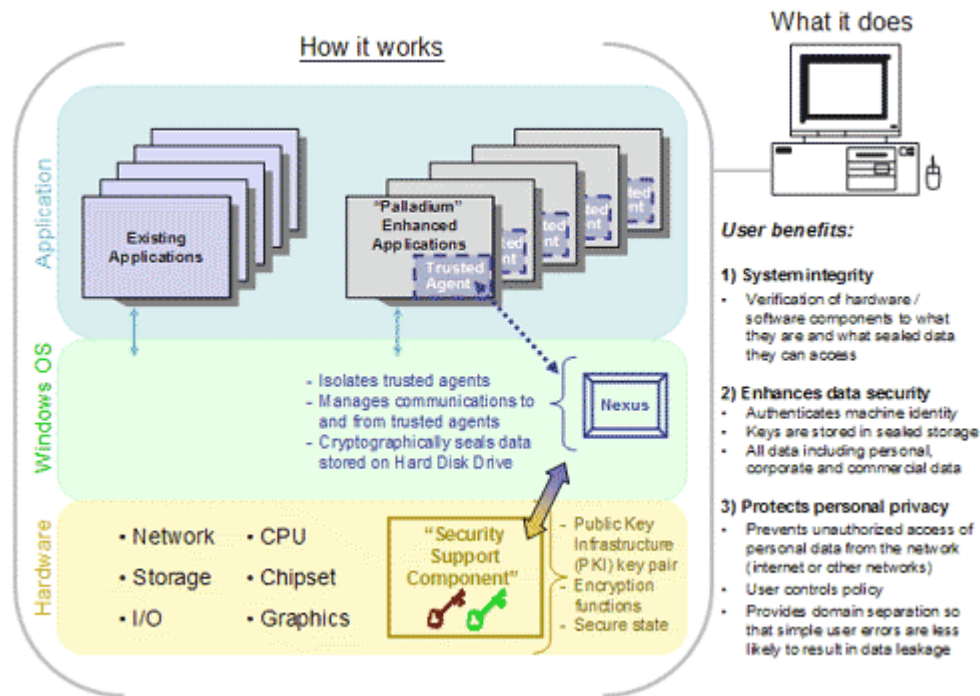


Figure 1: Palladium Architecture (Carroll A., et al)

COMPONENTS OF A PALLADIUM SYSTEM

Processor

To support Palladium, CPU manufacturers like Intel and Advanced Micro Devices (AMD) are developing new versions of their x86 chips. According to Geoffrey Strongin, platform security architect for AMD, these chips support a new "Trusted" execution mode that allows cryptographically authenticated programs access to a separate memory area (Boutin).

Security Coprocessor

The security coprocessor is one of the more interesting aspects of the TCGA/Palladium system. In the TCGA specification, the security coprocessor is referred to as a Trusted Platform Module (TPM). In the Microsoft specification, the TPM is referred to as the Security Support Component (SSC). The TPM is essentially a special kind of Smartcard. Its main job is to enhance system security. One of its functions is to generate a set of unique cryptographic keys that uniquely identify the system hardware. It contains these keys in a sealed memory space, and the keys themselves are never revealed to anyone. In addition, the TPM has several cryptographic algorithms that will be described later on. The TPM needs to ensure the integrity of components in the system and report this information to the operating system. In order to do this, it uses eight different 32-bit registers, called PCR[0] to PCR[7], that store eight different values of system measurements (Wintermute). These measurements are shown below (Wintermute):

- PCR[0]: Logs all the BIOS executable code and system's firmware.
- PCR[1]: Refers to CPU microcode updates, peripheral configuration in the platform, CMOS and ESCD (Extended System Configuration Data) if it exists, and SMBIOS (System Management BIOS, information over peripherals and their serial numbers, over the BIOS, physical and cache memory, slots, etc).

- PCR[2]: Option ROM code, that is, executable read-only memory from non-booting peripherals such as a graphic card. If it's a booting peripheral, it will be hashed as IPL code, and not as Option ROM.
- PCR[3]: Option ROM data and configuration.
- PCR[4]: IPL code, that is, booting-up code; i.e., for a hard disk the IPL would be the MBR code.
- PCR[5]: Configuration and IPL data, that is, i.e., for a hard disk this would be the partition table.
- PCR[6]: State transition (Events like sleeping)
- PCR[7]: Reserved

The TPM works by initializing every register with a known sequence in the beginning, and every time that a new element needs to be attached to the sequence, a hash algorithm will be performed over the concatenation of the sequence and the new value. Then, the data in the PCR registers contains information on the trusted hardware components in the system. Whenever an external system should request data from the PCR registers, the data is signed with a private key known only to the TPM. The reason for this is that the external components can be assured that the data really does come from the TPM. Every request to the TPM is assigned a random value. This way the external system can be assured that the TPM is answering exactly the request it was asked to answer (Wintermute).

There are several cryptographic algorithms that are present in the hardware of the TPM. The first of which is the SHA-1 Hash algorithm. It used for system integrity

measurements that are stored in the PCR logs. The second is RSA encryption. RSA encryption has several uses: a private key can sign the data TPM provides to the external world. Also, this algorithm is used to sign data that when it's needed to verify the TPM identity, and to encrypt/decrypt data and sub-tree crypto-keys (Wintermute). The third is RNG semi-random number generation. It is used against replication attacks (replicating a known request by a trusted component to the TPM). It tries to accomplish randomness by using a hash function over semi-random data. The implementation of the random seed is proposed to be temperature measurements or key presses. It is known that Palladium differs from the TCGA specification in that the TPM in a Palladium system will not be involved with authentication at boot time. Both specifications will require an operating system to use the TPM for the previously stated functions (Wintermute).

Vaults

With Palladium, Microsoft has named its secure data storage places "vaults". The vaults may reside on the user's computer or they may be third parties. Microsoft calls these third-party elements agents (Levy). These agents promise the ability to distribute just the specific details that a user wants revealed to the proper people. Microsoft employees have nicknamed the vault/agent management services "My Man" (Levy). Other parties interested in the information contained in the vaults would, upon user authorization, talk to the "Man" to receive the data.

Nexus

The Nexus is essentially a kernel component that controls system calls on programs running under Palladium and stores critical data from these programs. The Nexus would protect the memory zone where the kernel is kept, and the encrypted data held from applications and other user information. The Nexus seems like any other kernel implementation, in that it is inside a part of the memory that's protected from user processes; not physically isolated from the common memory but with a standard memory protection. It is suggested that the Nexus will rely heavily on the newer processors from Intel and AMD for trusted execution and memory protection.

ADVANTAGES OF PALLADIUM

Block Malicious Code

One of the more promising aspects that Palladium will bring to end-users is the ability to authenticate the programs they use. A user will allow certain applications access to resources. Originally, it was thought that Palladium would not permit unauthorized code to run on a system; therefore it would stop the execution of programs like viruses. Recently, however, Microsoft has backed off these claims about Palladium. Now it simply claims that Palladium will provide a secure execution environment for anti-virus programs (MS Palladium Technical FAQ). The benefit of a secure environment is that viruses and other malicious code cannot alter the behavior of a Palladium-enabled anti-virus program. Microsoft

has decided that legacy support for existing Windows applications is important enough so as not to require all programs to be rewritten for Palladium. This means that existing programs and viruses will still run on a Palladium system. The implied benefit to Palladium, aside from the added protection to anti-virus programs, is the increased authentication with new Palladium enabled programs. If Palladium proliferates as Microsoft hopes, there will come a time when legacy support will not be important anymore, and unauthorized programs will not be run. It appears as though this is the first step on the way to that idea.

Digital Rights Management

The digital rights management (DRM) potential with a Palladium system is what content producers and distributors are interested with. Digital rights management has to do with controlling whom and how long content is distributed. Microsoft touts Palladium as being independent of any existing DRM technology today (MS Palladium Technical FAQ). On the other hand, it acknowledges that Palladium systems are being designed to coincide with DRM technologies to help content developers (MS Palladium Technical FAQ). A Palladium system is supposed to make it easier for individual users to implement DRM on their own personal data. For example, a user may setup a vault containing credit card information. Palladium would allow the user to setup a group of trusted agents that would have access to all or certain parts of that data. Along with data, Palladium promises to give users the option to regulate time interval that data is available to the trusted agents they have specified.

DISADVANTAGES OF PALLADIUM

Upgrades

In order to take advantage of what Palladium is supposed to offer, users will have to upgrade both their current operating systems and hardware. The next version of Windows, due out in 2004, will need hardware support for Palladium features to work at all (MS Palladium Technical FAQ). It is unclear at this point whether the next major Windows release will run on non-Palladium compatible hardware. The central processing unit will have to support the trusted execution mode that Palladium offers. It is clear that future motherboards will need to contain the security chip for Palladium to run properly (MS Palladium Technical FAQ). More upgrades may be of concern in the area of graphic hardware and peripherals such as keyboards and mice because of the encryption in between these hardware devices and the software they are interacting with.

Interoperability

Palladium has received wide criticism for being a so-called General Public License (GPL) killer (Anderson). Now, Microsoft clearly states that the Palladium-enabled operating system will be able to co-exist with any Linux based system, just as their operating systems do today. The question that comes to mind is, will that change with wide spread adoption of the Palladium architecture? For example, if a bank switches over to exclusively Palladium systems, would customers of that bank who don't run Palladium systems be able to use the bank's services? Palladium is not

a direct attack on the GPL or Linux based systems, but it is an attempt to change the rules of the game.

Legacy Programs

By Microsoft's own admission, the Palladium-enabled operating system will not have perfect legacy support (MS Palladium Technical FAQ). All existing debuggers will need to be updated in order to work under Palladium. Performance tools that monitor operating system or user processes will need to be updated. Any memory dump software will not work correctly without changes to support Palladium. Hibernation features of motherboards will need to be updated as well. Memory scrub routines, at the hardware level, will need to be rewritten to accommodate Palladium. The reason for all of these updates is the trusted agent policy that Palladium enforces. No program is allowed to invade the execution space for any other program. In the case of a debugger, it will need special permission from the operating system to monitor the execution space of the target program. Even software developed for the TCPA specification will need to be rewritten if it tries to directly write to any TCPA hardware. This description of incompatible legacy programs is by no means comprehensive; it is simply what Microsoft is disclosing at this time (MS Palladium Technical FAQ).

CONCLUSION

The Internet and the proliferation of digital content have sparked the need for more privacy and security of data. The looming question whenever anyone talks about security and privacy is: for whom? Palladium certainly gives digital content

providers the control over their product that they have wanted for a long time. In recent months, Microsoft has clearly emphasized the benefits that the marriage of Palladium and DRM can bring to end-users. Microsoft claims that users will have complete control of their personal information. The Palladium-enabled operating system isn't due for at least another year. It could take months after the initial release for anyone to feel its effects. It is clear, however, that widespread adoption of Palladium will fundamentally change how we use our personal computers. The question is, will this change be for the better or the worse? Only time will tell.

BIBLIOGRAPHY

- Anderson, R. "TCPA / Palladium Frequently Asked Questions Version 1.0." July 2002. University of Cambridge Online. 5 Jan 2003
<<http://www.cl.cam.ac.uk/users/rja14/tcpa-faq.html>>.
- Arbaugh, Bill. "Improving the TCPA Specification." Aug. 2002. Ed. Institute of Electrical and Electronics Engineers (IEEE). Online., 2002.
- Boutin, Paul. "Palladium: Safe or Security Flaw?." 12 Jul. 2002. Wired News Online. 31 Jan 2003
<<http://www.wired.com/news/antitrust/0,1551,53805,00.html>>.
- Carroll A., et al. "Microsoft 'Palladium': A Business Overview." Aug. 2002. Microsoft Corporation Online. 5 Jan. 2003
<<http://www.microsoft.com/presspass/features/2002/jul02/0724palladiumwp.asp>>.
- Chan D., et al. "Trusted Computing Platform Alliance Main Specification Version 1.1b." 22 Feb 2002. Trusted Computing Platform Alliance Online. 5 Jan 2003
<http://www.trustedcomputing.org/docs/main%20v1_1b.pdf>.
- Hachman M., and Rupley S. "Microsoft's Palladium: A New Security Initiative." 25 Jun. 2002. ExtremeTech Online. 5 Jan 2003
<<http://www.extremetech.com/article2/0,3973,274309,00.asp>>.
- Lemos, R. "Security Technologies Could Backfire Against Consumers." 7 Nov. 2002. CNET News Online. 5 January 2003
<http://news.com.com/2009-1001-964628.html?tag=fd_lede1_hed>.
- Levy, Stephen. "The Big Secret." *Newsweek* 1 Jul. 2002; 48-50.
- Manferdelli, J. "Q&A: Microsoft Seeks Industry-Wide Collaboration for Palladium Initiative." 1 Jul. 2002. Microsoft Corporation Online. 5 Jan. 2003
<<http://www.microsoft.com/PressPass/features/2002/jul02/07-01palladium.asp>>.
- "Microsoft Palladium." 11 Nov. 2002. Electronic Privacy Information Center Online. 5 January 2003
<<http://www.epic.org/privacy/consumer/microsoft/palladium.html>>.
- "Microsoft Palladium Initiative - Technical FAQ." Aug. 2002. Microsoft Corporation Online. 5 Jan. 2003
<<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/>>

security/news/PallFAQ2.asp>.

Mundie C., et al. "Trustworthy Computing Whitepaper." Oct. 2002. Microsoft Corporation Online. 5 Jan. 2003
<<http://www.microsoft.com/presspass/exec/craig/10-02trustworthywp.asp>>.

"TCPA Design Philosophies, Version 1.0." 25 Jan. 2001. Trusted Computing Platform Alliance Online. 5 Jan 2003
<http://www.trustedcomputing.org/docs/designv1_0final.pdf>.

"TCPA Frequently Asked Questions, Rev 5.0." 3 Jul. 2002. Trusted Computing Platform Alliance Online. 5 Jan 2003
<http://www.trustedcomputing.org/docs/Website_TCPA%20FAQ_0703021.pdf>.

"Trustworthy Computing From Fingertips to Eyeballs: Roundtable Highlights Fundamental Shift in Approaches to Secure and Private Computing." 18 Nov. 2002. Microsoft Corporation Online. 5 Jan. 2003
<<http://www.microsoft.com/presspass/features/2002/nov02/11-18twcroundtable.asp>>.

Wintermute. "TCPA and Palladium Technical Analysis Version 1.07." 25 Jan. 2003. 1 Feb. 2003
<<http://wintermute.homelinux.org/miscelanea/TCPA%20Security.txt>>.