Content Security
Business Unit

Microsoft Palladium: A Business Overview

Combining Microsoft Windows Features, Personal Computing Hardware, and Software Applications for Greater Security, Personal Privacy, and System Integrity

by Amy Carroll, Mario Juarez, Julia Polk, Tony Leininger

Microsoft Content Security Business Unit

June 2002

Legal Notice

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred.

Abstract

"Palladium" is the codename for an evolutionary set of features for the Microsoft® Windows® operating system. When combined with a new breed of hardware and applications, these features will give individuals and groups of users greater data security, personal privacy, and system integrity. In addition, Palladium will offer enterprise customers significant new benefits for network security and content protection. This white paper:

- Examines how Palladium satisfies the growing demands of living and working in an interconnected, digital world.
- Catalogs some of the planned benefits offered by Palladium.
- Summarizes the software components of Palladium.
- Presents a suggested broad business approach to enable Palladium to succeed.

Contents

The Challenge: Meeting the Emerging Requirements of an Interconnected World

Today's personal computing environment has advanced in terms of security and privacy, while maintaining a significant amount of backwards compatibility. While abandoning compatibility and many features over the years might have made possible smaller, faster, and/or more trusted systems, personal computer users required the preservation of investments in software, hardware, and user training that came with backwards compatibility.

However, the evolution of a shared, open network (the Internet) has created new problems and requirements for trustworthy computing. For example, the proliferation of private information within a digital, networked world is creating a growing challenge. As the personal computer grows more central to our lives at home, work, and school, consumers and business customers alike are increasingly aware of privacy and security issues.

Now, the pressure is on for industry leaders to:

- 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 backwards compatibility with existing software and user knowledge that exists with Windows systems today.
- Together, industry leaders must address these critical issues to meet the mounting demand for trusted computing while preserving the open and rich character of current computer functionality.

The Solution: Palladium

"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 users 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.

Users implicitly trust their computers with more of their valuable data every day. They also trust their computers to perform more and more important financial, legal, and other transactions. Palladium provides a solid basis for this trust: a foundation on which privacy- and security-sensitive software can be built.

There are many reasons why Palladium will be of advantage to users. Among these are enhanced, practical user control; the emergence of new server/service models; and potentially new peer-to-peer or fully peer-distributed service models. The fundamental benefits of Palladium fall into three chief categories: greater system integrity, superior personal privacy, and enhanced data security. These categories are illustrated in Figure 1.

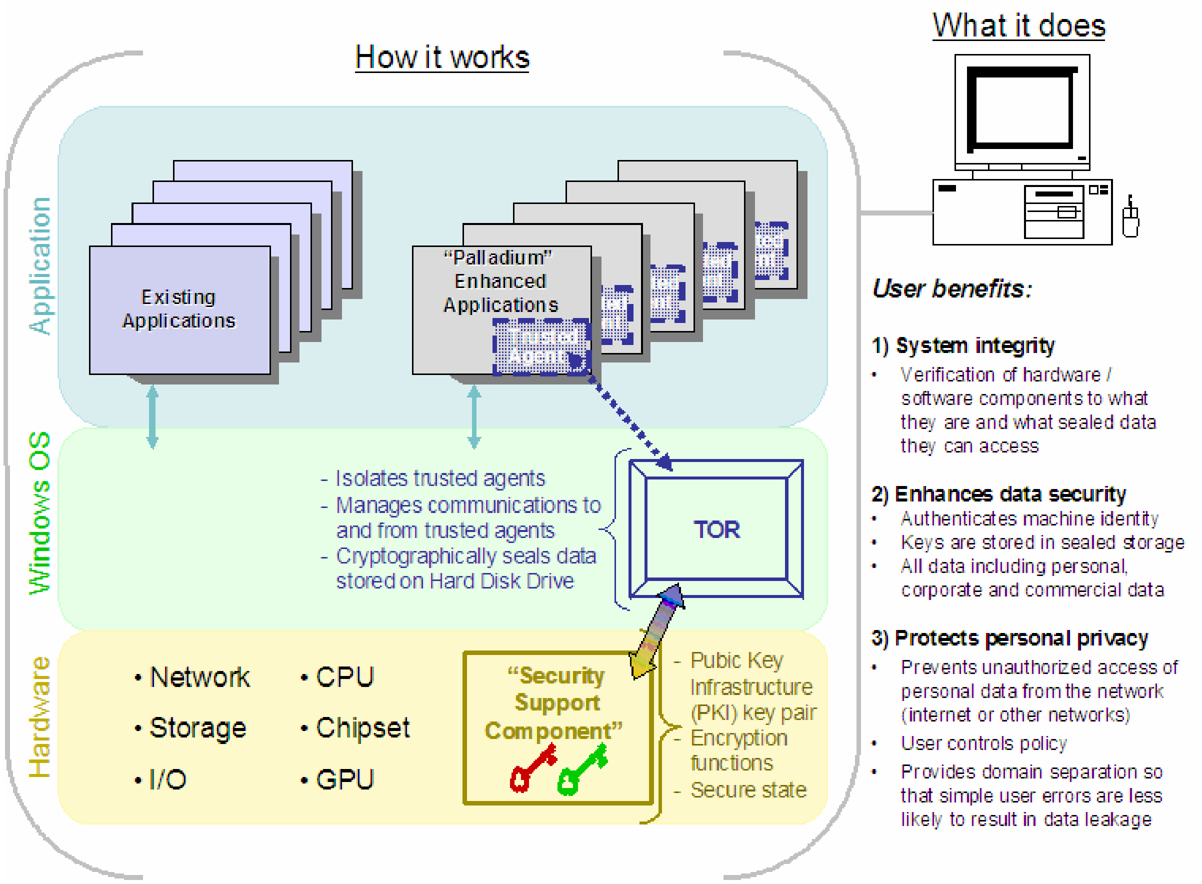
How it works
Application
Windows OS
Hardware
Existing Applications
"Palladium" Enhanced Applications
Trusted Agent
- Isolates trusted agents
- Manages communications to and from trusted agents
- Cryptographically seals data stored on Hard Disk Drive
TOR
• Network
• Storage
• I/O
• CPU
• Chipset
• GPU
"Security Support Component"
- Pubic Key Infrastructure (PKI) key pair
- Encryption functions
- Secure state
What it does
User benefits:
1) System integrity
• Verification of hardware / software components to what they are and what sealed data they can access
2) Enhances data security
• Authenticates machine identity
• Keys are stored in sealed storage
• All data including personal, corporate and commercial data
3) Protects personal privacy
• Prevents unauthorized access of personal data from the network (internet or other networks)
• User controls policy
• Provides domain separation so that simple user errors are less likely to result in data leakage

Figure 1: Windows-based personal computer of the future.

Core Principles of the Palladium Initiative

Development of Palladium is guided by important business and technical imperatives and assumptions. Among these are the following:

A Palladium-enhanced computer must continue to run any existing applications and device drivers.

Palladium is not a separate operating system. It is based on architectural enhancements to the Windows kernel and to computer hardware, including the CPU, peripherals, and chipsets, to create a new trusted execution subsystem (see Figure 1).

Palladium will not eliminate any features of Windows that users have come to rely on; everything that runs today will continue to run with Palladium.

In addition, Palladium does not change what can be programmed or run on the computing platform; it simply changes what can be believed about programs, and the durability of those beliefs. Moreover, Palladium will operate with any program the user specifies while maintaining security.

It is important to note that while today's applications and devices will continue to work in Palladium, they will gain little to no benefit from Palladium services. To take advantage of Palladium, existing applications must be adapted to utilize the Palladium environment or new applications must be written. This software—whether a component of a Microsoft Win32®-based application or a new application—is called a "Trusted Agent."

Palladium-based systems must provide the means to protect user privacy better than any operating system does today.

Palladium prevents identity theft and unauthorized access to personal data on the user's device, while on the Internet and on other networks. Transactions and processes are verifiable and reliable (through the "attestable" hardware and software architecture described below), and they cannot be imitated.

With Palladium, a system's secrets are locked in the computer and are only revealed on terms that the user has specified. In addition, the trusted user interface prevents snooping and impersonation. The user controls what is revealed and can separate categories of data on a single computer into distinct "realms." Like a set of vaults, realms provide the assurance of separability. With distinct identifiers, policies, and categories of data for each, realms allow a user to have a locked down work environment and fully open surfing environment at the same time, on the same computer.

Finally, the Palladium architecture will enable a new class of "identity" service providers that can potentially offer users choices for how their identities are represented in online transactions. These service providers can also ensure that the user is in control of policies for how personal information is revealed to others. In addition, Palladium will allow users to employ identity service providers of their own choosing.

Palladium will not require digital rights management (DRM) technology, and DRM will not require Palladium.

DRM is an important, emerging technology that many believe will be central to the digital economy of the future. As a means of defining rules and setting policies that enhance the integrity and trust of digital content consumption, DRM is vital for a wide range of content-protection uses. Some examples of DRM are the protection of valuable intellectual property, trusted e-mail, and persistent protection of corporate documents.

While DRM and Palladium are both supportive of Trustworthy Computing, neither is absolutely required for the other to work. DRM can be deployed on non-Palladium machines, and Palladium can provide users with benefits independent of DRM. They are separate technologies. That said, the current software-based DRM technologies can be rendered stronger when deployed on Palladium-based computers.

User information is not a requirement for Palladium to work.

Palladium authenticates software and hardware, not users. Palladium is about platform integrity, and enables users—whether in a corporate or a home setting—to take advantage of system trustworthiness to establish multiple, separate identities, each to suit specific needs.

For example, an employee logs onto the corporate network from home. A trusted gateway server at the corporate network mediates the remote access connection, allowing only trusted applications to access the network. This assures that the network is protected against infection from attacks by viruses that the home user might have received through personal e-mail. Once connected, the employee can use Remote Desktop to access the computer at the office or save a file back to the corporate server by using locally active Trusted Agents and sealed storage (see below) on the client.

With this technology, the corporate network is protected while the individual can also be confident that the company is not using the remote connection as an opportunity to snoop into the contents of the user's home computer.

Palladium will enable closed spheres of trust.

A "closed-sphere-of-trust" binds data or a service to both a set of users (logon) *and* to a set of acceptable applications. As shown in Figure 2, the Trusted Operating Root (TOR) does not simply open the vault; the TOR will only open a particular vault, and only for a small list of applications.

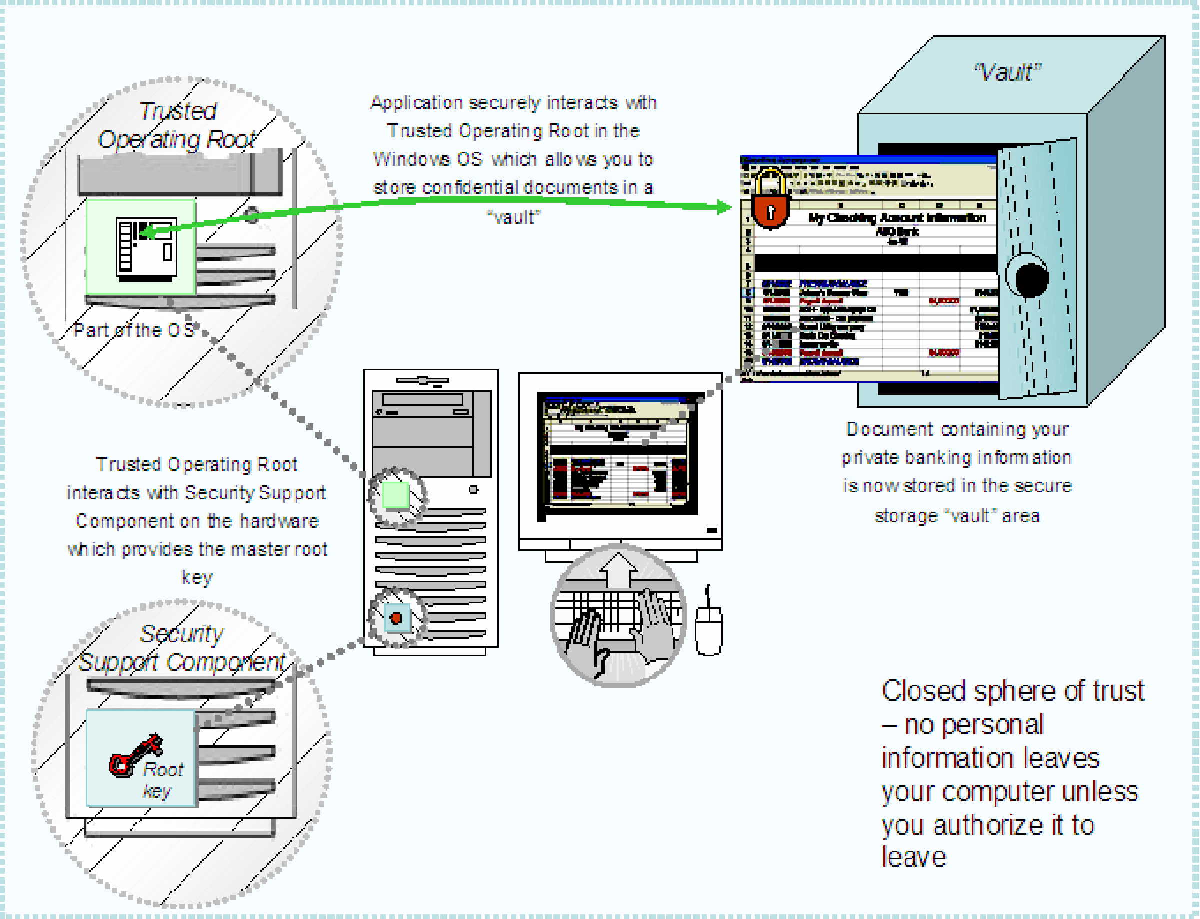
Trusted Operating Root
Part of the OS
Application securely interacts with Trusted Operating Root in the Windows OS which allows you to store confidential documents in a "vault"
"Vault"
My Checking Account Information
Document containing your private banking information is now stored in the secure storage "vault" area
Trusted Operating Root interacts with Security Support Component on the hardware which provides the master root key
Security Support Component
Root key
Closed sphere of trust – no personal information leaves your computer unless you authorize it to leave

Figure 2: Closed Sphere of Trust.

Palladium is an opt-in system.

Palladium is entirely an opt-in solution; systems will ship with the Palladium hardware and software features turned off. The user of the system can choose to simply stay with this default setting—leaving all Palladium-related capabilities (hardware and software) disabled.

Turning Palladium completely off includes turning it off in hardware, which prevents any software from turning it back on. Users have the ultimate control over their systems and their information; Palladium does not entail any global requirements.

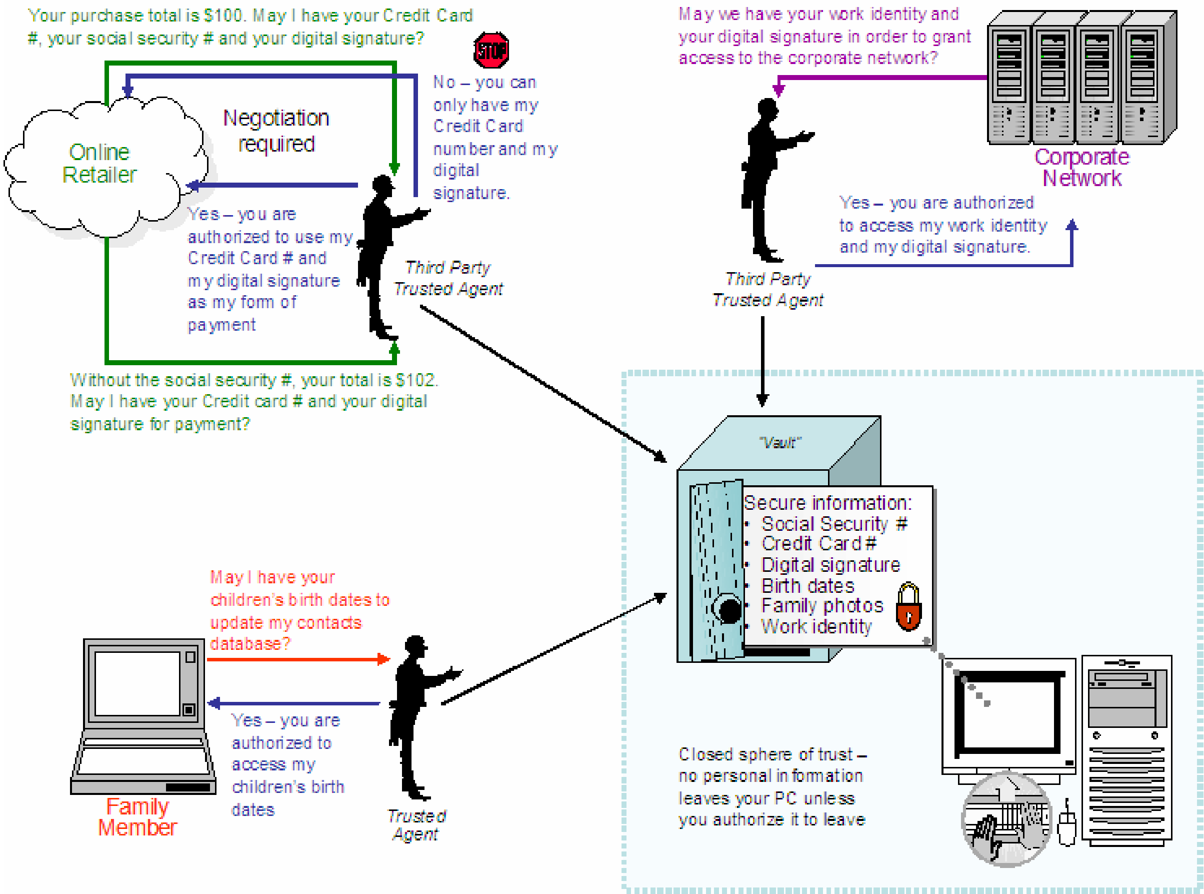
Your purchase total is $100. May I have your Credit Card #, your social security # and your digital signature?
STOP
Online Retailer
Negotiation required
No – you can only have my Credit Card number and my digital signature.
Yes – you are authorized to use my Credit Card # and my digital signature as my form of payment
Third Party Trusted Agent
Without the social security #, your total is $102. May I have your Credit card # and your digital signature for payment?
May we have your work identity and your digital signature in order to grant access to the corporate network?
Corporate Network
Yes – you are authorized to access my work identity and my digital signature.
Third Party Trusted Agent
"Vault"
Secure information:
Social Security #
Credit Card #
Digital signature
Birth dates
Family photos
Work identity
May I have your children's birth dates to update my contacts database?
Yes – you are authorized to access my children's birth dates
Family Member
Trusted Agent
Closed sphere of trust – no personal information leaves your PC unless you authorize it to leave

Figure 3: Palladium Scenarios.

Palladium must be highly resistant to software attacks (such as Trojan horse viruses), and must provide users with the integrity of a protected, end-to-end system across networks.

Palladium provides a trusted processing environment. Trusted code runs in memory that is physically isolated, protected, and inaccessible to the rest of the system, making it inherently impervious to viruses, spy-ware, or other software attacks.

One of the key Palladium building blocks is "authenticated operation." If a banking application is to be trusted to perform an action, it is important that the banking application has not been subverted. It is also important that banking data can only be accessed by applications that have been identified as trusted to read that data. Palladium systems provide this capability through a mechanism called "sealed storage."

Another capability provided by authenticated operation is "attestation." Palladium will allow a bank to accept only transactions initiated by the user and that are not viruses or other unknown machines on the Internet. Because Palladium software and hardware is cryptographically verifiable to the user and to other computers, programs, and services, the system can verify that other computers and processes are trustworthy before engaging them or sharing information. Users can therefore be confident that their intentions are properly represented and carried out, as illustrated in Figure 3. Moreover, the source code for the operating system's critical TOR will be published and validated by third parties.

Finally, interaction with the computer itself is trusted. Palladium-specific hardware provides a protected pathway from keyboard to monitor and keystrokes cannot be snooped or spoofed, even by malicious device drivers.

Palladium data security features will make a Windows-based device a trustworthy environment for any data.

The Palladium system is architected with security and integrity as its primary design goals. Trusted code cannot be observed or modified when running in the trusted execution space. Files are encrypted with machine-specific secrets, making them useless if stolen or surreptitiously copied. In addition, machine-specific system secrets are physically and cryptographically locked (the machine's private key is embedded in hardware and never exposed), and the trusted hardware architecture prevents snooping, spoofing, and data interception. Core system secrets are stored in hardware, where no software attack can reveal them. Even if exposed by a sophisticated hardware attack, the core system secrets are only applicable to data on the compromised system and cannot be used to develop widely deployable hacks. Finally, a compromised system can likely be spotted by IT managers, service providers, and other systems, and then excluded.

A Palladium system will be open at all levels.

Palladium hardware will run any TOR. Some platforms may allow a user to restrict the TORs that are allowed to run, but the user will still be in full control of this policy. The Palladium TOR will also run trusted agents from any publisher. Again, the user may choose to restrict the trusted agents that run on the system, but the user will remain in full control of this policy. The Palladium TOR will work with any network service provider of the user's choosing.

Aspects of Palladium

Palladium comprises two key components: hardware and software.

Hardware Components

Engineered for ensuring the protected execution of applications and processes, the protected operating environment provides the following basic mechanisms:

- **Trusted space:** An execution space that is protected from external software attacks such as a virus. Trusted space is set up and maintained by the TOR and has access to various services provided by Palladium, such as sealed storage.
- **Sealed storage:** 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. Information in sealed storage cannot be read by other non-trusted programs. (Sealed storage cannot be read by unauthorized secure programs, for that matter, and cannot be read even if another OS is booted, or the disk is carried to another machine.) These stored secrets can be tied to the machine, the TOR, or the application. We will also provide mechanisms for the safe and controlled backup and migration of secrets to other machines.
- **Attestation:** A mechanism that allows the user to reveal selected characteristics of the operating environment to external requestors. For example, attestation can be used to verify that the computer is running a valid version of Palladium.

These basic mechanisms provide a platform for building distributed trusted software.

Software Components

The platform implements these trusted primitives in an open, programmable way to third parties. The platform consists of the following elements:

- **Trusted Operating Root (TOR):** The component in Microsoft Windows that manages trust functionality for Palladium user-mode processes (agents). The TOR executes in kernel mode in the trusted space. 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.
- **Trusted agents:** A trusted agent is a program, a part of a program, or a service that runs in user mode in the trusted space. A trusted agent calls the TOR 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 TOR. One of the main principles of trusted agents is that they can be trusted or not trusted by multiple entities, such as the user, IT department, a merchant or a vendor. Each trusted agent or entity controls their own sphere of trust, and they need not trust or rely on each other.

Together, the TOR and trusted agents provide the following features:

- **Trusted data storage:** Encryption services for applications to ensure data integrity and protection.
- **Authenticated boot:** Facilities to enable hardware and software to authenticate itself.

From the perspective of privacy (and anti-virus protection) one of the key benefits of Palladium is the ability for users to effectively delegate certification of code. Anyone can certify Palladium hardware or software, and we expect that many companies and organizations will offer this service. Allowing multiple parties to independently evaluate and certify Palladium-capable systems means that users will be able to obtain verification of the system's operation from organizations that they trust. Additionally, this will form the basis for a strong business incentive to preserve and enhance privacy and security.. Moreover, Palladium allows any number of trusted internal or external entities to interact with a trusted component or trusted platform.

Business Approach

Microsoft recognizes that in order for a long-term undertaking of this magnitude to be successful, we must be proactive about sharing information and doing business in new ways. We plan to develop Palladium as a collaborative consumer and industry initiative. This means the following:

- We are dedicated to working as transparently as possible, ensuring that a wide range of stakeholders are fully aware of and, to the extent possible, significantly involved in the development process.
- In order to gather all perspectives and ensure that a broad range of voices contributes to the Palladium initiative, we are engaging major influentials and organizations including, but not limited to, those concerned with privacy, security, consumer advocacy, public interest, and government issues.
    - Our product development process will include steps to implement this key stakeholder feedback.
    - We plan to provide a roadmap that will publicly define opportunities for broad input.
- We are working intensively with hardware companies to ensure comprehensive offerings and widely available support when Palladium is launched.
- We will engage major customers to develop solutions that will meet critical business needs.
- We will take significant and public measures to ensure the trustworthiness, authenticity, and integrity of the fundamental elements of Palladium prior to launch. These measures include:
    - A plan to publish the source code of the TOR.
    - All Palladium functionality will be turned off by default. This puts control over all features in the hands of the customer (or at the customer's request, an OEM or service provider) to choose to opt-in.
    - A plan to examine the Palladium architecture on a regular basis by a credible security auditor.
    - The receipt of as many seal-of-approval endorsements as possible from credible organizations to certify the quality of Palladium and the veracity of our claims.

Timing

Palladium is a long-term endeavor. The first Palladium-enhanced personal computers will not appear on the market for several years, and we do not foresee widespread adoption for some years after the introduction. However, now is the time to begin planning for—and working on—Palladium.

Conclusion

Today, IT managers face tremendous challenges due to the inherent openness of end-user machines, and millions of people simply avoid some online transactions out of fear. However, with the usage of Palladium systems, trustworthy, secure interactions will become possible. This technology will provide tougher security defenses and more abundant privacy benefits than ever before. With Palladium, users will have unparalleled power over system integrity, personal privacy, and data security.

Independent software vendors (ISVs) who want their applications to take advantage of Palladium benefits will need to write code specifically for this new environment. A new generation of Palladium-compatible hardware and peripherals will need to be designed and built. The Palladium development process will require industry-wide collaboration. It can only work with broad trust and widespread acceptance across the industry, businesses, and consumers.

Palladium is not a magic bullet. Clearly, its benefits can only be realized if industry leaders work collaboratively to build Palladium-compatible applications and systems—and then only if people choose to use it. But the Palladium vision endeavors to provide the trustworthiness necessary to enable businesses, governments and individuals to fully embrace the increasing digitization of life.

For More Information

To learn more about Palladium, send e-mail to the Palladium information alias (pdinfo@microsoft.com).

For more information on Microsoft products and security, see the Microsoft Security page at the Microsoft Web site (http://microsoft.com/security).

For more information on Microsoft products and privacy, see the Microsoft Privacy page at the Microsoft Web site (http://microsoft.com/privacy).

For more information about the Windows operating system, see the Microsoft Windows page at the Microsoft Web site (http://microsoft.com/windows).