Microsoft Palladium

Aarohi Patel
121006

Introduction

"Palladium" is the code name for an evolutionary set of features for the Microsoft Windows operating system. Palladium is a system that combines software and hardware controls to create a "trusted" computing platform.

When combined with a new breed of hardware and applications, this feature can give individuals and groups of users greater

- Data security
- Personal privacy
- System integrity

Palladium can offer enterprise customers significant new benefits for network security and content protection.

Need for Palladium

The growth of Internet has created an increasing need of trustworthy computers, reliability and integrity. There is a demand for trusted computing while preserving the open and rich character of current computer functionality. Designed to work side-by-side with the existing functionality of Windows, this significant evolution of the personal computer platform would introduce a level of security that meets the rising customer requirements for data protection, integrity and distributed collaboration.

The main advantages of Palladium to the users are enhanced, practical user control; the emergence of new server/service models; and potentially new peer-to-peer or fully peer-distributed service model. The functional benefit of Palladium falls into three main categories: greater system integrity, superior personal privacy and enhanced data security.

Technology

Two key components of Palladium are:

Hardware Components

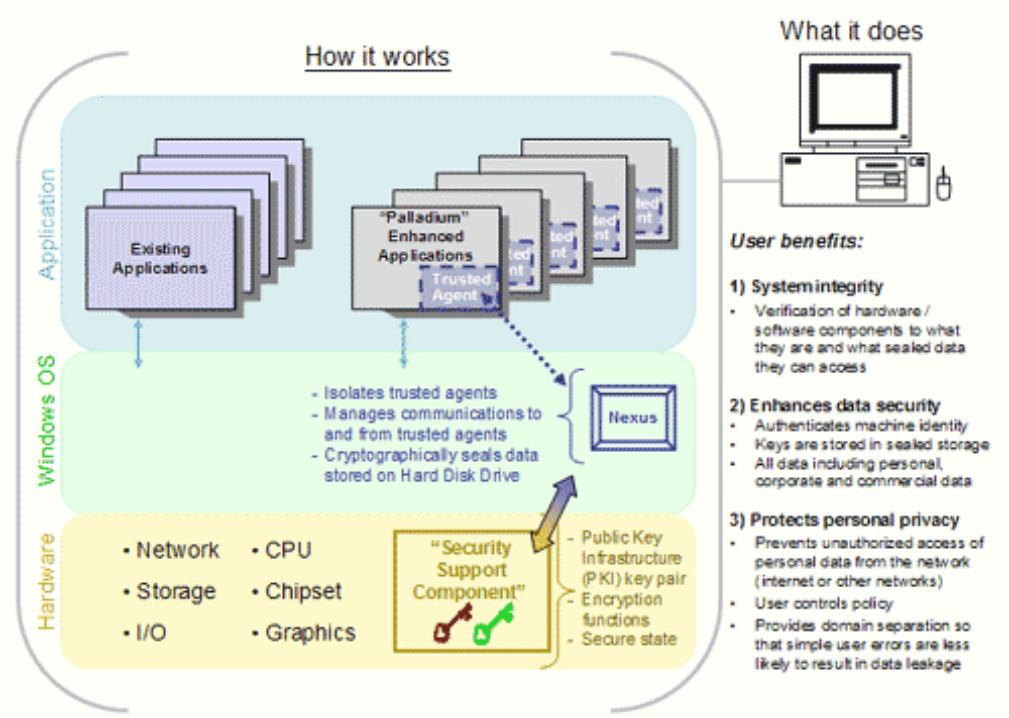
Engineered for ensuring the protected execution of applications and processes, the protected operating environment provides the following basic mechanisms:

- **Trusted space:** The execution space is protected from external software attacks such as a virus. Trusted space is set up and maintained by the nexus and has access to various services provided by "Palladium," such as sealed storage.
- **Sealed storage**: Sealed storage is 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. Other non-trusted programs cannot read information in sealed storage. (Sealed storage cannot 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.) These stored secrets can be tied to the machine, the nexus or the application. Microsoft will also provide mechanisms for the safe and controlled backup and migration of secrets to other machines.
- **Attestation:** Attestation is 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."

Software Components

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

- **Nexus (a technology formerly referred to as the "Trusted Operating Root (TOR)":** The component in Microsoft Windows that manages trust functionality for "Palladium" user-mode processes (agents). The nexus 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 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. 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



Together, the nexus 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

ADVANTAGES

Some of its advantages are:

1. Information is Secure: Palladium stores all personal data on our home machine and not on server. We have to explicitly allow someone to have access to that data. The great part about the setup is that all information is centralized and under our direct control.
2. Open Source and Palladium: Palladium is a conservative extension of PC. Thus it won't disable any operating systems that run on the PC. In fact, it's possible for Linux or FreeBSD to implement a Nexus and run its own trusted apps.
3. No user Authentication: There is no user authentication with Palladium. It is the software's job to authenticate the user, not part of the Palladium specification. The software can be trusted because it is verified by the hardware.

DISADVANTAGES

1. Upgrades
2. Legacy Programs
3. Break Once Break Everywhere (BOBE)
4. Attack Vectors

REFERENCES

https://epic.org/privacy/consumer/microsoft/palladium.html

http://en.wikipedia.org/wiki/Next-Generation_Secure_Computing_Base

White paper on “Microsoft Palladium”