Microsoft Palladium

Aarohi Patel(121006)

Introduction

- "Palladium" is the code name for an evolutionary set of features for the Microsoft Windows operating system
- A set of hardware and software extensions to make the PC more trustworthy.
- This feature can give individuals and groups of users greater
  - Data security
  - Personal privacy
  - System integrity

Technology

Hardware Components

- **Trusted space:** 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

- **Attestation:** Attestation is a mechanism that allows the user to reveal selected characteristics of the operating environment to external requestors.

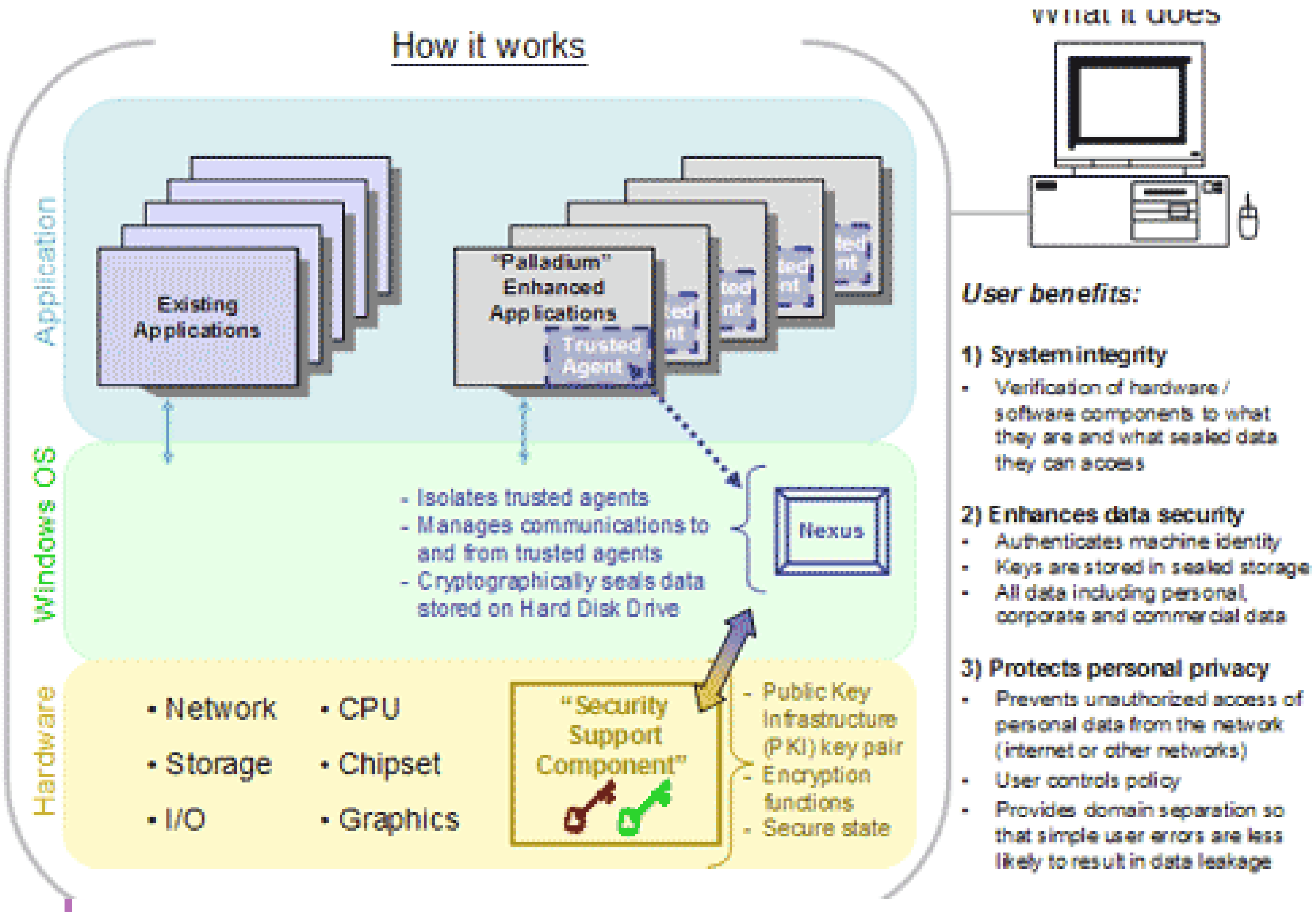
+

Software Component

- **Nexus (a technology formerly referred to as the "Trusted Operating Root (TOR)"**
- **Trusted agents**

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



- Isolates trusted agents
- Manages communications to and from trusted agents
- Cryptographically seals data stored on Hard Disk Drive

- Public Key Infrastructure (PKI) key pair
- Encryption functions
- Secure state

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

How the system work

+

ADVANTAGES

- Information is Secure
- Open Source and Palladium
- No user Authentication

DISADVANTAGES

- Upgrades
- Legacy Programs
- Break Once Break Everywhere (BOBE)
- 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”