ISSN No. 0976-5697

Volume 5, No. 4, April 2014 (Special Issue)

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Advanced Network Security with Palladium

B.Ramana Reddy[1], M.Susmitha[2], B.Sireesha[3]
[1,2,3]Dept. of Computer Science & Engineering
Annamacharya institute of Tech. & sciences, Tirupati, India

Abstract: Security in this contemporary scenarios has become a more sensible issue either it may be in the real world or in the Cyber World. In the real world as opposed to the cyber world an attack is often preceded by information gathering. Movie gangsters case the joint; soldiers "scout the area". This is also true in the cyber world. Here the "bad guys" are referred to as intruders, eavesdroppers, hackers, hijackers, etc. The intruders would first have a panoramic view of the victis network and then start digging the holes. Today the illicit activities of the hackers are growing by leaps and bounds, viz., The recent attack on the DNS servers has caused a lot of hullabaloo all over the world". However, fortunately, the antagonists reacted promptly and resurrected the internet world from the brink of prostration. Since the inception of conglomerating Computers with Networks the consequence of which shrunk the communication world, hitherto, umpteen ilks of security breaches took their origin. Tersely quoting some security ditherers – Eavesdropping, hacking, hijacking, mapping, packet sniffing, 1spoofing, dos & ddos attacks, etc. Newton's law says "Every action has got an equal but opposite reaction". So is the case with this. nevertheless the security breaches and eavesdroppers, the technological prowess has been stupendously developed to defy against each of the assaults. Our paper covers the advanced technical combats that have been devised all through the way, thus giving birth to the notion of Network -Security. Various antidotes that are in fact inextricable with security issues are – cryptography, authentication, integrity and non repudiation, key distribution and certification, access control by implementing firewalls etc. To satiate the flaws in the network security more and more advanced security notions are being devised day by day. Our paper covers a wide perspective of such arenas where the contemporary cyber world is revolving around viz., palladium cryptography. Palladium is a content protection concept that has spawned from the belief that the pc, as it currently stands, is not architecturally equipped to protect a user from the pitfalls and challenges that an all-pervasive network such as the internet poses. In the course of this paper the revolutionary aspects of palladium are discussed in detail. A case study to restructure the present data security system of jntu examination system using palladium is put forward.

Keywords: Palladium, Security, Cryptography, Attack, Eavesdropping

I. INTRODUCTION

Microsoft is working with chip partners **Intel**, **AMD** and others on a technology code-named Palladium that would make security and privacy features a standard component of the future Windows-based PC.

Ultimately, the Palladium technology would be incorporated on desktop PCs, servers and handhelds. It would offer security and system integrity down to the hardware level, enabling users to establish more secure and "provable" relationships with other users and systems beyond the corporate firewall.

The Palladium technology will, for example, offer unique security APIs designed by Microsoft for third-party software vendors and Microsoft's own product groups, to exploit for application and server software development.

Software giant Microsoft today leaked the first bits of information about a comprehensive security scheme called "Palladium" -- named after a statue of the goddess Athena (also called Pallas) which guarded the gates of the legendary city of Troy.

II. ADVANCED SECURITY NOTION – PALLADIUM "A REVOLUTIONARY BREAK THROUGH IN DATA SECURIYTY"

Palladium is the code name for a revolutionary set of "features" for the "windows" operating system. The code name of this initiative –"palladium", is a Moniker drawn from the Greek mythological goddess of wisdom and protector of civilized life.

Till date most forms of data security have been software oriented with little or no hardware involvement. Palladium can be touted as the first technology to develop software-hardware synchronization for better data security. Hardware changes incorporated by palladium are reflected in the key components of the CPU, a motherboard chip (cryptographic co-processor), input and output components such as the graphics processor etc.

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 consumers significant new benefits for network security and content protection.

A. Core principles of the palladium initiative:

Palladium is not a separate operating system. It is based in 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.

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" environment or new applications must be written.

In addition, palladium does not change what can be programmed or run on the computing platform. Palladium will operate with any program the user specifies while maintaining security.

III. ASPECTS OF PALLADIUM

Palladium comprises two key components: hardware and software.

A. *Hardware components:*

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

a. ***Trusted Space:*** (or curtained memory). This is an execution space that is protected form 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. In other words it is protected R.A.M.

b. ***Sealed Storage:*** Sealed storage is an authenticated mechanism that allows a program to store secrets that cannot be retrieved by un trusted programs such as a virus or Trojan horse. Information in sealed storage can't be read by other un trusted programs (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 of the application. Palladium will also provide mechanisms for the safe and controlled backup and migration of secrets to other machines. In other words it is a secured and encrypted part of the hard disk.

c. ***Secure input and output:*** A secure path from the keyboard and mouse to palladium applications and a secure path from palladium applications to the screen ensure input-output security.

d. ***Attestation:*** Attestation is a mechanism that allows the user to reveal selected characteristics of the operating environment to external requestors. In reality it takes the form of an encryption co-processor. It is entrusted with the job of encryption and decryption of data "to and from" the "sealed storage".

B. *Software components:*

The following are the software components of palladium:

Nexus (a technology formerly referred to as the "trusted operating root (TOR)") This component 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 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.

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.

IV. WORKING OF PALLADIUM

Palladium is a new hardware and software architecture. This architecture will include a new security computing chip and design changes to a computer's central processing unit (CPU), chipsets, and peripheral devices, such as keyboards and printers. It also will enable applications and components of these applications to run in a protected memory space that is highly resistant to tempering and interference.

The pc-specific secret coding within palladium makes stolen files useless on other machines as they are physically and cryptographically locked within the hardware of the machine. This means software attacks can't expose these secrets. Even if a sophisticated hardware attack were to get at them, these core system secrets would only be applicable to the data within a single computer and could not be used on other computes.

V. PROTECTION USING PALLADIUM

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 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 choice.

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 it is expected 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. In addition, 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.

VI. SHORTCOMINGS AND PIT FALLS OF PALLADIUM

Though palladium can provide a higher degree of much needed data security it is not without its share of problems like:

a. Software and applications have to be rewritten to synchro- nize with palladium or new applications must be written.
b. Changes are to be made to the existing computer hardware to support palladium.
c. It would be a long time before this technology became common place.

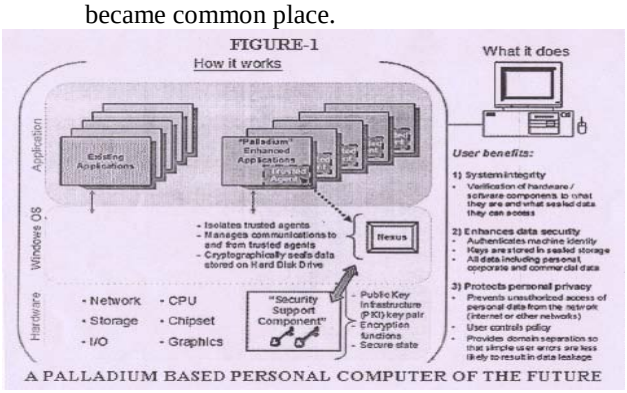

Figure 1: Working of Palladium

VII. CASE STUDY

A. Restructuring Data Security Of Jntu Examination System Using Palladium:

a. Existing system: In order to eliminate the leakage of question papers, the Jawaharlal Nehru technological university (J.N.T.U), Hyderabad, has recently decided to implement the system of Electronic Distribution of Examination Papers (EDEP) – a new method of conducting the examinations.

In this system, 4 sets of question papers are generated and encrypted into a " college-specific" C.D.

The encrypted CD is supplied to the examination centers about 3 days in advance.

The question papers in encrypted form are also made available on the JNTU examination website.

Password to read the CDs is supplied one hour before the commencement of examination to the principal/chief superintendent through internet, cell phone, telephone or Fax.

The principal soon after receipt of password decrypts the original question papers of that day using the software supplied by JNTU examination branch.

The EDEP employs the method of public key cryptography.

Though this system is largely stable and secure it has certain loopholes like:

a) As the encrypted question papers are also available on the Internet there is every chance of crackers downloadi-ng and trying to decrypt them.
b) This method of 4 sets of question papers has been resented by the student and teacher community alike.
c) There is every chance of failure or mis-match of the college specific C.D., due to the large number of affiliate colleges (as is been observed in some cases).
d) Also, in one case, a previous examination C.D. was mistakenly decrypted, and the question papers thus printed, distributed initially at an examination center.

B. Palladium-as a solution (as shown in figure 2):

Palladium is based on the concept of trusted space. A closed sphere of trust binds data or a service, to both a set of users and to a set of acceptable applications. Due to this an unauthorized user cannot access the data or software which is based on a server.

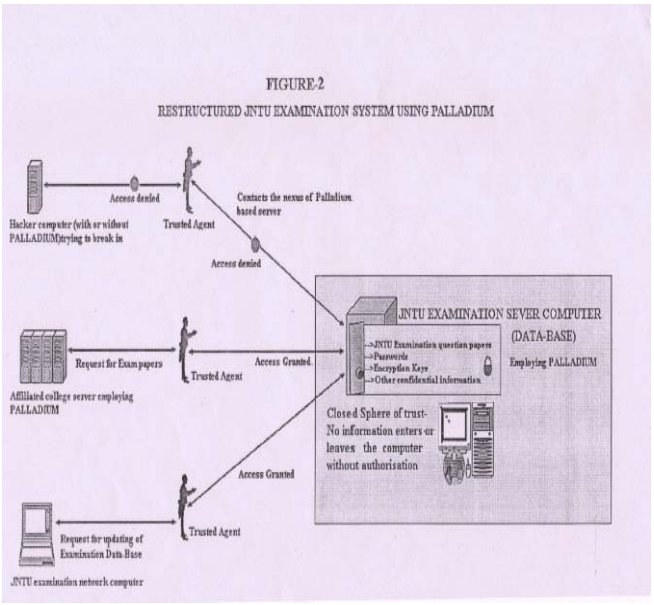

Figure 2: Solution of JNTU Examination System by using Palladium

In the revised system the encrypted question papers are put up on the J.N.T.U's palladium based server and all the affiliate colleges use college-specific palladium computers. It works as follows:

a. A third party trusted agent (government or private programmed) is employed who is responsible for granting of access to JNTU examination server. It processes the requests and forwards only those certified by the "nexus" of the JNTU's palladium based server.
b. If an unauthorized system (without palladium) forwards a request it is immediately rejected by the server's trusted agent. Even if an unauthorized palladium PC tries to access the server its request is rejected.
c. The PC-specific secret coding within palladium makes stolen files useless on other machines as they are physically and cryptographically locked within the hardware of the server or trusted computer.
d. During examinations the palladium computer of the college issues a request to the common trusted agent (of JNTU and college) via internet. This request is granted and each-particular question paper pertaining to that day is accessed by the college.

C. Advantages:

a. As the process of question paper down load is highly secure, the chances of leakage are literally nil.
b. Since this method is highly trustworthy a single set question paper system can be employed.

c. An advanced system of Internet communication can be adopted for a broader reach, thus eliminating the role of C.D.
d. Since the download of question papers is "request-specific and time bound" there can not be a case of question paper mis-match.

D. Denoument:

The capability of security enabled components still lags behind the claims. Basic security challenges in the corporate realm are not yet completely addressed. Nevertheless the cumbersome combats devised against each of the security fissures, yet the cyber MAVERICKS all around the world are succeeding in their ways of perdition. This was quite evident from the E-attacks on BARC server & post-September11th cyber attacks on FBI sites where even sophisticated surveillance systems couldn't come to their rescue.

A case in point is that, E-ATTACKS are becoming notoriously peerless as compared with the traditional nuke-wars. Consequently, in the quench of thirst for more and more secured systems "BIOMETRIC SYSTEMS, QUANTUM-CRYPTOGRAPHY" and many more are innovatively being implemented at a cumulative pace.

If we are not exaggerating, lets be optimistic of a 100% foolproof, SECURED global village in the near future. Don't Forget Newton's laws say "Every action has got an equal but opposite reaction".

VIII.REFERNCES

[1] Power, Richard. 2002 CSI/FBI Computer Crime and Security Survey. Computer Security Institute. 2002.

[2] Pearson, Preneel, and Proudler. Trusted Computing Platforms: TCPA Technology in Context. Prentice Hall PTR, ISBN: 0130092207, 1st edition, July 22, 2002.

[3] Presentation at MIT Lab for Computer Science on Trusted Computing Platform Alliance by Joe Pato of HP Labs, 17 October 2002.

[4] Presentation at MIT Lab for Computer Science on An Overview of Palladium by Brian A. LaMacchia of Windows Trusted Platform Technologies, 17 October 2002.

[5] http://www.computereconomics.com/article.cfm?id=133

[6] http://www.howstuffworks.com/virus2.htm

[7] http://www.oreillynet.com/pub/a/wireless/2012/05/24/wlan.html

[8] http://www.cf.ac.uk/infos/guides/legislation/copyright/Fair_dealing.pdf

[9] http://in.news.yahoo.com/021010/14/1w8xk.html

[10] http://www.jntu.com