Palladium Cryptography Palladium Cryptography Next Generation Security Computation Base

Harshwardhan Rathore, Asst. Prof. Pushpanjali M. Chouragade

Abstract— In today's world when man is mostly dependent on gadgets for his work, security is a topic which can't be ignored. In this paper we will be dealing a new cryptographic technique known as Palladium Cryptography which deals with the change in the basic hardware architecture to facilitate security. We will be looking at the various architectural modifications and will be describing the hardware and software components in depth. We will discover the working mechanism of palladium. We will also explore the various uses of palladium followed by its cons and will end up with a conclusion.

1 INTRODUCTION

Cryptography comes from two Greek words which mean 'Hidden Writing'. It comes from the times of Julius Caesar, when he used to communicate with his generals using 'Caesar Cipher'. In it, each letter in the plaintext was replaced by a letter some fixed number of positions further down the alphabet.

In simple language, Cryptography is a way of converting plain text into specially coded text known as Cipher text. This Cipher text can be converted back to the original text only by special programs or software which is available with authorized people only. Even if an intruder steals that data he won't be able to make use of that data without the key to this cipher text.

2 PALLADIUM

For papers Palladium (also known as Next Generation Secure Computing Base) is a software architecture designed by Microsoft to implement TRUSTED COMPUTING in the newer versions of Microsoft's Windows operating system. Palladium relies on hardware technology designed by members of Trusted Computing Group(TCG), which provides a number of security related features like fast random number generation, cryptographic co-processor ,etc. Both these software and hardware modifications made to the current architecture will collectively result in greater data security and personal privacy to an individual user as well as an organization.

3 ARCHITECTURAL DETAILS

A complete Palladium based will consist of both software as well as hardware components. Most of the features used in palladium are heavily based on the specialized hardware modifications.

There are two hardware components; the Trusted Platform Module(TPM),which provides secure storage for cryptographic keys, a secure cryptographic co-processor and a curtained memory feature in the Central Processing Unit (CPU).

The software components include the Nexus, a security kernel that is a part of the operating system and provides a secure environment called as the Nexus mode which helps in running trusted code. Also there are Nexus Computing Agents (NCAs) which are trusted services or programs which run in the Nexus mode.

We must remember that Palladium is not a separate operating system but a set of enhancements done to the Windows kernel. Thus we can say that any programs running on the machine today will be running with palladium as well. No features of the Windows will be eradicated while using Palladium.

Only the programs which are going to be run on the machine are needed to be tweaked in order to run with Palladium. Also we must note that all the programs which could be programmed today, will be able to be programmed with Palladium as well.

4 HARDWARE COMPONENTS

- Trusted Platform Module

The Trusted Platform Module(TPM) is used to hold the secret Cryptographic Key. This key is stored in the Trusted Platform Module during the time of manufacturing and is never passed on to any other component of the system, even not to the owner. Surprisingly it is very difficult to retrieve the Cryptographic Key even through reverse engineering or any other method.

Trusted applications will pass encrypted data based on this cryptographic key to be decrypted by the trusted platform module. The Trusted Platform module will decrypt this data only under strict conditions and after the decryption this data will only be passed to trusted applications making it inaccessible to other applications and operating systems. This decrypted data will only be stored in the curtained memory and nowhere else.

The Trusted Platform Module also generates Cryptographic Signature based on its Cryptographic Key. This signature may be verified by any other third party which may be in a network with the system for remote attestation and to verify that the data being received is secure.

- Curtained Memory

Curtained Memory is an execution space provided by the central processing unit. Data decrypted by the Trusted Platform module residing in this curtained memory can only be ac-

cessed by the trusted application to which it belongs and not to any other application or operating system. Applications are verified that if or not they are Trusted Applications using the attestation feature provided by the Trusted Platform Module. This attestation is confirmed by checking if these applications are running in Curtained Space or not.

5 SOFTWARE COMPONENTS

- If you are using Nexus

The Nexus is the main component which manages trust functionality between various applications which are running simultaneously on the system. The Nexus runs as a security kernel and provides various services like establishment of new process, attestation of applications and sealing and unsealing of secrets.

- Nexus Computation Agents (NCAs)

A Nexus Computing Agents is a program or part of a program which has been attested by the Nexus. It runs in the curtained memory in the Nexus mode. The Nexus Computing Agents request the Nexus for security related services like for communicating between other trusted applications. These agents are allowed to store their data in the curtained memory while their computation and are able to identify themselves as trusted applications using the attestation feature implemented by the Trusted Platform Module via the Nexus.

6 WORKING OF PALLADIUM

Palladium uses software as well as hardware architectural modifications in order to provide better security. The physical modification incorporates the Trusted Platform Module chip which is used to hold the cryptographic key of the computer and is also used to attest various applications which will run on the system. As virus and malwares are also a small piece of code which we call a program, will need some space to execute in the system. But the Trusted Platform Module won't attest them as trusted applications as they are unknown to the system. As the curtained space is only provided to the trusted applications these virus and malwares won't get their share of curtained space and hence they won't be able to run in the curtained space and won't be able to steal any secret data from the system.

All the encoding and decoding business done under palladium is pc-specific. All the data encrypted or decrypted is done on the basis of the cryptographic key stored in the Trusted Platform Module. Like every lock has a unique key, these encrypted files can be decrypted by the same cryptographic key with which it was encrypted. Hence, even if in case, some secret files are even stolen from the system by any means they are useless for the intruder as these files are physically as well as cryptographically locked in the hardware of the system. By this we can say that any software attacks done to the system won't be able to hamper the security of the system and won't reveal any secrets stored on the machine.

6.2 How Palladium Is Useful

Palladium was a part of the implementation of Trusted Computing which will make computers safer, less prone to viruses and malwares and hence much more reliable than today. When seen from the user's perspective it will prevent identity theft and unauthorized access to personal data which are the most common threats we are facing today.

All the secrets are stored in the machine and can be only revealed as per the specification of the user. The user can separate files and programs according to any scheme as per his convenience and also can specify access rights to each individual program. For example he may lockdown all the programs which can access his mail ids and keep other programs like games and music players unlocked. So the data related to the programs which can access the mail ids of the user is stored only in the curtained memory and can be accessed only by those programs. Whereas the data of the unlocked applications which is not of much importance to the user can be accessed by other unauthorized applications too.

Also the user connected to a network can restrict the limit to which his personal information and identity will be revealed to the other users of the network. In this ways all the online transactions will be safer and there will be less cases of snooping and impersonation.

6.3 Problems Associated With Palladium

As it is said a coin has two faces, similarly every technology has its pros and cons. The upside is the security it provides to the users. But every facility has its price to be paid. The various problems associated with it are:-

- Palladium requires many modifications to be done to the basic hardware architecture of the machine which is time consuming and increases the cost factor.
- All the applications which are to run on the machine are needed to be rewritten in order to synchronize with palladium hence increasing development cost.
- Existing software and hardware will also run and work respectively with Palladium but they won't provide very less or no security featured by Palladium.

4 CONCLUSION

We saw many aspects of palladium and tried to understand it from its root till its end. We started with the Introduction describing what is Cryptography followed by a brief explanation of what Palladium is and what it does. We then explored the Architectural aspects of Palladium followed by the in depth specification of the various hardware as well as software modifications which are to be done in Palladium. We then discovered how Palladium works and how it is useful to its end users. In the end we also discussed its pitfalls.

In the end I feel that Palladium has a lot to offer to us and I also feel that it is also capable of keeping its promises. Looking at today's computer centric world and the threats associated with it I feel that Palladium can solve most of these problems.

I do agree that the modifications that are to be done to the existing software and hardware will be cumbersome and would lead to increase in the manufacturing cost. But while glancing to the facilities and security that Palladium offers I feel it is worth every penny.

In the upcoming days of my research I will be trying to eradicate the problems of Palladium and I believe that Palladium will be the new face of data security.

REFERENCES

[1] Palladium Cryptography: an Advanced Data Security. http://www.scribd.com/doc/37054599W.-K. Chen, *Linear Networks and Systems*. Belmont, Calif.: Wadsworth, pp. 123-135, 1993. (Book style)

[2] Cryptography - Wikipedia, http://en.wikipedia.org/wiki/cryptography

[3] , Next-Generation Secure Computing Base http://en.wikipedia.org/wiki/nex-generation-secure-computing-base

[4] Random number generation http://en.wikipedia.org/wiki/randomnumbergeneration

[5] Aman Sagar and Sanjeev Kumar Palladium in Cryptography: The Advancement in Data Security. HCTL Open Int. J. of Technology Innovations and Research HCTL Open IJTIR, Volume 7, January 2014 e-ISSN: 2321-1814 ISBN (Print): 978-1-62951-250-1.