Palladium Cryptography : A security perspective

Krishna Das[1], Akankshya Patel[2], Manisha Kachhap[3]

[1,2,3]Department of IT, C. V. Raman College of Engineering[123]
krishnadas7018@gmail.com[1], akankshya.patel000@gmail.com[2], manishakachhap60@gmail.com[3]

Abstract—In today's life we basically dependent on mostly gadgets in which the security system is very important and necessary. That's why we are dealing a new techniques which is known as palladium cryptography. Palladium Cryptography is a software architecture which is a secure computing system based for next generation for security purpose. This cryptography gives a large number of security related features such as fast random number generation, keys for secure cryptography which makes them difficult or almost impossible to get it back. We will be looking at the various architecture modifications and we will be describing the hardware and software components in depth.

Index Terms—Cryptography, Palladium, Network Security

I. INTRODUCTION

Cryptography comes from two Greek words which means 'Hidden Writing'. It comes from the times of Julius Caesar, when he used to communicate with his generals using 'Caesar Cipher'. In this, 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 which is known as Cipher text. It 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.

II. ARCHITECTURE DETAILS

A complete Palladium Cryptography 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 such as TPM which is known as trusted platform module. It provides the secure storage for cryptographic keys. This cryptographic co-processor and a curtained memory feature in the central processing unit.

The software components include the Nexus, a security kernel which is the part of the operating system and provides a secure environment called as the Nexus mode. It helps in running trusted code. Palladium is not a separate operating system but a set of enhancements done to the windows kernel. Nexus is the main component which manages trust functionality between various applications.

III. WORKING OF PALLADIUM

Palladium uses software as well as hardware architectural modifications in order to provide better security and better performance. The physical modification incorporates the Trusted Platform Module (TPM) 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 they won't be able to run in the curtained space and won't be able to steal any secret data or information from the system.

IV. HOW PALLADIUM IS USEFUL

Palladium is a part of implementation of Trusted Computing which will make computers safer and protects from virus and malwares and much more reliable. All the secrets are stored in the machine and it can be only revealed as per the specification of the user.

The user connected to a network which can restrict the limit to 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.

V. PROBLEM 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:-

1- Palladium requires many modifications to be done to

the basic hardware architecture of the machine which is time consuming and this is also increases the cost factor.

2- All the applications which are able to run on the machine are needed to be rewritten in order to synchronize with palladium hence increasing development cost.

3- Existing software and hardware it will also run and work respectively with Palladium but they won't provide very less or no security featured by palladium.

VI. ADVANTAGES

1- One of the most promising aspects that palladium will bring to end user is the ability to authenticate the programs which they use.

2- The process of question paper download is very highly secure and safe, the chances of leakage are literally very less or we can also say that it is nil.

VII. DISADVANTAGES

Software and applications have to be rewritten to synchronize with palladium. Changes are to be made to the existing computer hardware to support palladium. It would be a long time before this technology becomes commonplace

VIII. CONCLUSION

In this paper we discussed about the basics of cryptography and we also know about the working principle of this type of cryptography. By this type of cryptography the security system is so high.

REFERENCES

[1]https://www.google.co.in/search?q=palladium+cryptography+is+a+software+or+hardware&oq=palladium+cryptography+is+a+software+or+hardware&aqs=chrome..69i57.19334j0j7&sourceid=chrome&ie=UTF-8

[2] http://ijtir.hctl.org/vol7/IJTIR_Article_201401004.pdf

[3] Haripriya Rout, Brojo Kishore Mishra, "Pros and Cons of Cryptography, Steganography and Perturbation techniques", 2014 National Conference on Network security (NCNS 2014), College of Applied Science, Adoor, Kerala, 5 & 6 December 2014, published in IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), e-ISSN: 2278-2834, p- ISSN: 2278-873, PP 76-81.