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

Palladium in Cryptography: The Advancement in Data Security

***Aman Sagar**[*] **and Sanjeev Kumar**[†]*
asgr19oct@gmail.com and sksanju792@gmail.com

Abstract

This paper deals with the basics of Cryptography, it's essential features and categories and three different types of keys used by the two categories of cryptography. It also deals with deals kinds of ciphers which are used in both old and modern cryptography methods. The main aim of this paper is to pinpoint the idea of palladium which is used in the modern era of cryptography and how it helps us in the network security.

Keywords

Cryptography, Palladium, Decryption, Network Security, Drawbacks of Palladium.

[*]Department of Computer Science and Engineering, FST, The ICFAI University, Dehradun, India
[†]Department of Computer Science and Engineering, FST, The ICFAI University, Dehradun, India

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

Introduction

Palladium Cryptography is a software architecture which is a secure computing base for next generation. It 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.

An Overview Of Cryptography

Key Concepts and Terminology

Cryptography

The word `Cryptography` is originated from Greek which means secret writing. It is a based on the concept of science and the art of transforming messages to make them immune to attack and making it more secure.

PlainText and CipherText

The original message before its transformation is called `PlainText`. Once the message is transformed, it is called `CipherText`.

Key

The Key is a set of numbers in which cipher operates. To encrypt the message, there are three requirements i.e. encryption algorithm, an encryption key and the `plaintext`.

Categories of Cryptography

There are two categories of cryptography algorithms or ciphers i.e. symmetric key (also known as secret-key) and asymmetric key(also known as public key).

Symmetric-Key Cryptography

In symmetric-key cryptography, the key is shared and the same key is used by the sender (for encrypting the data) and receiver (for decrypting the data).

e-ISSN: 2321-1814
ISBN (Print): 978-1-62951-250-1

Asymmetric-Key Cryptography

In asymmetric-key cryptography, two keys are used i.e. private and public key. The private key is used by the receiver for decrypting the data and the public key is used by the sender for encrypting the data.

Modern Ciphers

The ciphers used in the modern era is called round ciphers as they involve multiple rounds and each round is a complex cipher which consists of many simple ciphers.

Data Encryption Standard

It was designed by IBM and then adopted by U.S government as the standard encryption method for non-military and non-classified use. The algorithm encrypts a 64-bit plaintext by using a 64-bit key.

Advanced Encryption Standard

The main reason for the introduction of AES is that DES keys were too small and the process for encryption and decryption in DES was too slow. AES is designed with three key sizes: 128, 192 and 256 bits.

Why Security is Needed?

Most of the companies contain valuable information which needs to be protected. As, now a day's data and information of the organizations are stored in the computers so that security of these computers play a major role. So, the protection of these information against unauthorized usage becomes major and primary concern for operating systems as well as for users.

Threats for Data

The three general goals and their threats from a security point of view to the computer system are:

1. `Data Confidentiality` is the first goal to be achieved for the security of data. The data should remain secret and should be visible only to the people who have the authority for it and the system should maintain the integrity that the unauthorized person can't access the data.

e-ISSN: 2321-1814
ISBN (Print): 978-1-62951-250-1

2. `Data Integrity` is the second goal which means without the permission of the owner, the users are not allowed to make modifications in it. Data modification not only mean to making any changes in the data but also to removing the data and adding incorrect information to it.

3. `System Availability` is the third goal which ensures that the system can't be disturbed by anyone to make it unstable. It must ensure that the data should be accessed by the authorized persons and do not suffer the denial of service.

Palladium: An Invention in Data Security

Palladium is the set of features which created a revolution in the windows operating system. It is derived from the Greek mythology i.e. goddess of wisdom. Till now, the data security was purely software oriented with little or no hardware involvement. It is the first technology developed by the synchronization of hardware and software for the advancement in security.

The fundamental principles of Palladium are as follows:

1. Palladium is purely based on the enhancement of the architecture of the windows kernel and computer hardware such as CPU, peripherals etc.

2. It will not eradicate any functionality of the windows which the users are using currently. Whatever is running in the windows currently will be running exactly the same with palladium.

3. As the current era applications and devices will be deployed on palladium, then it might give some benefit to the applications from the palladium environment.

4. Palladium will operate on the program specified by the user defined while maintaining the security.

Components of Palladium

Palladium is based on two key components i.e. hardware and software.

Hardware Components

For ensuring the execution of the applications and processes, the mechanism followed by the protected operating environment is as follows:

e-ISSN: 2321-1814
ISBN (Print): 978-1-62951-250-1

1. `Trusted space`: Trusted space is the execution space which protects from external storage attacks such as virus. It is managed by the Nexus and has the authority to access the diversified services of palladium like sealed storage.

2. `Sealed storage`: It is the mechanism that allows a program to keep the data secured from the unauthorized programs such as viruses, Trojan horse etc. The unauthorized or non-trusted programs are not able to read the information kept in the sealed storage.

3. `Secure input/output`: To ensure the input/output security, secured path is followed by the keyboard and mouse for palladium applications.

4. `Attestation`: It provides a mechanism which allows users to use some characteristics of the operating system to external requirements.

Software Components

Software components of palladium are as follows:

`Trusted agents`: It is a sub program that runs in the user mode in trusted space. It calls nexus for security issues and critical general services such as memory management. The main idea behind the trusted agents is that it may or may not be trusted by multiple entities such as vendors, users etc.

The features provided by the nexus and trusted agents as a combined module is as follows:

1. Ensuring the data integrity to the encrypted services for applications and trusted data storage.

2. Providing facilities so that the hardware and the software can authenticate by its own.

How Palladium Works

Palladium is the new invention in the hardware and software architecture. It engulfs new computing chips, change in the design of the CPU, chipsets and other I/O devices. It provides a platform to components of these applications to run in a protected memory space which is extremely resistant of interference and tampering.

The files encrypted by the pc secret coding within palladium can't be modified in other devices as they are cryptographically locked in the machine in which it was stored. It tells that any software attacks can't harm the files.

Drawbacks in Palladium

Some pitfalls in the palladium is as follows:

1. It is mandatory for the software and applications to be re-written for the synchronization within palladium.

2. Modification is the primary requirement to be done in the existing computer hardware to support palladium.

Conclusion

In this paper, we have discussed about the basics of Cryptography, it's essential features, different categories of Cryptography and the ciphers used in these categories. We have looked to the concept of Palladium, its components, its working and some of its pitfalls.

For the future study in Palladium, I would look forward to eradicate the pitfalls and make it more effective.

References

[1] Palladium Cryptography: an Advanced Data Security. http://www.scribd.com/doc/37054599

[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] Ankur and Divyanjali, An Introduction to Pseudorandom Number Generator, HCTL Open International Journal of Technology Innovations and Research, Volume 4, July 2013, ISSN: 2321-1814, ISBN: 978-1-62776-132-1.

e-ISSN: 2321-1814
ISBN (Print): 978-1-62951-250-1 *References*

[6] Shaishav Agrawal, Amit Jaspal, Ankit Aggarwal, Ratna Sanyal and Sudip Sanyal, Hybrid Approach: A Solution for Extraction of Domain Independent Multiword Expressions, HCTL Open International Journal of Technology Innovations and Research, Volume 5, Sept 2013, ISSN: 2321-1814, ISBN: 978-1-62840-986-4.

[7] Amrit Suman, Mahesh Gour and Raksha Mehra, Cloud Computing: A Modern Art and its Research Challenges, Edition on Cloud and Distributed Computing: Advances and Applications, Volume 2 - August 2013 of HCTL Open Science and Technology Letters (STL), ISSN: 2321-6980, ISBN: 978-1-62840-833-1.

[8] Aman Sagar, Bineet Kumar Joshi and Nishant Mathur, A Study of Distributed Denial of Service Attack in Cloud Computing (DDoS), Edition on Cloud and Distributed Computing: Advances and Applications, Volume 2 - August 2013 of HCTL Open Science and Technology Letters (STL), ISSN: 2321-6980, ISBN: 978-1-62840-833-1.

[9] Shakti Dhar Tiwari, Mahesh Kumar and Preeti Mishra, Cloud Computing: Implementation of Software as a Service (SaaS) Multitenancy, Edition on Cloud and Distributed Computing: Advances and Applications, Volume 2 - August 2013 of HCTL Open Science and Technology Letters (STL), ISSN: 2321-6980, ISBN: 978-1-62840-833-1.

[10] Mahesh Kumar and Shakti Dhar Tiwari, Cloud Computing: Various Aspects of Cloud Security, Edition on Cloud and Distributed Computing: Advances and Applications, Volume 2 - August 2013 of HCTL Open Science and Technology Letters (STL), ISSN: 2321-6980, ISBN: 978-1-62840-833-1.