Cyber Security: DES Working And AES Working

Summary

The term Cyber is related to information technology. Cyber security is use for protecting the network, program, systems and mobile devices form digital attacks. The main purpose of attacks to access, change and destroy the sensitive data. Common methods mostly attackers used to access the network or computer to get sensitive data are viruses, worm, spyware and Trojans.

The information and technology industry has evolved greatly over the last half century. Over the last several years computer expert and computer polices makers concerns to protect the information and communication technology from cyber-attacks done by unauthorized persons. When we talk about cyber security infect we talk about data security. Any type of text, audio, video is called data.

There are two major types of data encryption one is DES and second is AES. Des is data encryption standard which use 56bit key to encrypt data. AES is Advance type of data Encryption which is developed in 2000. It can be implemented on various platforms especially in small devices. It is carefully tested for many security applications. AES use following steps to encryption sub bytes, shift Rows, Mix columns and add Round key but in final round mix column is not perform. Cyber security is big issue that affects persons as well as other none public and business industries. In past computer user were not worried about cyber security. But when the world makes a global thorough internet, users don’t understand the solution of security problems.

1. Introduction

Cyber security is well known term which is relate to internet. The term Cyber is related to information technology. When combine these two words cyber and security, gives the meaning of protection of information technology. Cyber security is use for protecting the network, system, program and mobile devices form digital attacks.

Attack is another term used in Cyber technology. The main purpose of attacks to access, change and destroy the sensitive data. There are many types of attacker but two are common one is hacker and second is cracker. Hacker is a person that use his skills to secure the network, mostly hackers are creative they create program to secure the network. But in other case crackers are not creative, they use copyright software. The main purposes of cracker destroy the network to get the sensitive information. Crackers do this job for money. This act is called cybercrime.

Common methods mostly attackers used to access the network or computer to get sensitive data are viruses, worm, spyware and Trojans. Viruses and worm are same like to viruses in human body, they are self-replicate which damage files. Trojans and spyware is like a spy, that means secretly collect the data.

1.1. Background of cyber security

In this age everyone who use computer is familiar with viruses and other attaching terms. Looking five years ago most of people who use computer did not think about the protecting their data. In 1949 the famous scientist Jon von Neumann published the self-reproducing Automata. This is first step of computer viruses. This theory is used by other people in development of self-replicating software. In 1960 engineer Paul gave new idea of communication network. In 1968 a new theory comes which is packet switching. According to this theory data can be send in small parts to make transmission easier. In 1969 Arpanet sends first message.

Arpanet is first packet switching network developed by US government. After two year in 1971 first computer viruses appear. It is called the Creeper virus. After this first Antivirus software is created to remove the virus from system. In the passage of time internet security changed in many ways. In this age there are many security risks.

1.2. Purpose of study

Purpose of this report is to study cyber security. The information and technology industry has evolved greatly over the last half century. Over the last several years computer expert and computer polices makers concerns to protect the information and communication technology from cyber-attacks done by unauthorized persons.

1.3. Method of study

I used the internet to collect the relevant information for this report. I consult some books and websites to gather information regard this report.

2. Discussion

When we talk about cyber security infect we talk about data security. Any type of text, audio, video is called data. For protection of data two encrypting method are used one is DES and second is AES. DES stands for data encrypting standards. Encryption is method to secure data step by step by using algorithms. DES is symmetric which use same keys in encryption and decryption and give data in cipher form. It accepts data in 64bit plane text and also use 56bit key to encryption of data. It use 16 rounds and in each round functional keys are used.

2.1. DES working

(64bit plane text 32bit left 32bit right Cipher 64bit plane text)

(Round 1 Round 16)

But DES is breakable system mostly DES used to secure unclassified data because unclassified data is not important. The advance form of data encryption standard is called AES (advance encryption standard). It is developed in 2000 and it is considered more secure then DES.

Advance encryption standard algorithm is not only for security but also for great speed. This is

also called new encryption standard. It uses 128, 192 and 256 bit keys. 128bit key perform 10 rounds, 192bit key use 12 rounds while 256bit key use 14 rounds to encrypt the data.

It can be implemented on various platforms especially in small devices. It is carefully tested for many security applications.

2.2. AES working

2.2.1. Step followed by AES

- These steps used to encrypt 128-bit block
- The set of round keys form the cipher key.
- Initialize state array and add the initial round key to the starting state array.
- Perform round 1 to 9 execute usual round.
- Execute final round
- Corresponding cipher text chunk output of final round steps to usual round.

2.2.2. Working

(128bit text Inverse shift rows)

(Sub Byte)(Add round key) (Mix columns) (Shift rows)

3. Finding

Cyber security is big issue that affects persons as well as other none public and business industries. In past computer user were not worried about cyber security. But when the world makes a global thorough internet, users don’t understand the solution of security problems.

In this age internet security is more important to protect the sensitive data. The result we deduct that cyber security is play key role in information technology. We should up to date with the passage of time with security laws and following simple steps of protections.

4. Conclusion

This report focused on the cyber security, in discussion section we see the data encryption standards and see the some important things which play important part in security but internet is very large field also we can say that whole world is on internet and perform different activities. Some people do good activities and some do bad activities. The people who perform bad activities on internet are danger for security. These people do not know what they are doing, they do things for their own shake, and they do everything which they interest.

But some people know what they are doing. They do bad activities for money. Mostly big organizations hire these people to defeat his enemy in business. With the passage of time we should check our internet activities. Also checks the important account on internet like mails and other things.

5. Recommendation

For security we should follow these points

· Strong password

Password is used to secure user data from unauthorized person. We should use strong password and with the passage of time change it. We should change our password in once a week.

· Backup data

To manage the security always use backup of your data. Unfortunately when you lost your data can use backup data.

· Firewall

Always activate the firewall of the system. Firewall protects the user to unauthorized access of other people/devices.

· Security software

Use some security software to protect your computer from threads. Antivirus is best example of security software that protect computer from threads.

6. References

1. Cyber Security: Problems and Solutions. (2018, May 14). Retrieved from http://www.glowtouch.com/cybersecurity-problems-and-solution/
2. What is cyber security? What you need to know. (n.d.). Retrieved from https://us.norton.com/internetsecurity-malware-what-is-cybersecurity-what-you-need-to-know.html
3. What Is Cybersecurity? (n.d.). Retrieved from https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html