IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

COMPUTER SECURITY

Kulkarni Pratiksha S., Jaid Swati D., Nilakh Ashwini B., Miss.Pawar M.R.
Information Technology, Jaihind Polytechnic,Kuran, India.

ABSTRACT

Computer security is like a vital organ of Computer system.It cannot be ignored for thye safety purpose of computer security.Main goal of computer security is to prevent computer system from threats.There are many types of threats for computer system like hacking of mails,any confidential data,passwords,bank accounts.Computer security is like lock for door,to stop the thieves to come in house.computer security prevents the threats to effect the computer system.Computer hacking is well known issue as well as growing day by day in computer networking and internetworking. To overcome this issue and to provide security to the computer in our network we have to concentrate on its security and prevent hackers and thefts from accessing our important as well as confidential data.

KEYWORD: Hacking,Hackers,safeguards,Eavesdropping,Spoofing,Cryptography.

INTRODUCTION

Computer Security is one of the main part of the computer field.Nowadays Computer is used in Every field like bank,colleges,hospitals,scools,offices,etcIn every field computer security is required to protect the data. Some of the computer threats are hacking,Spoofing,Eavesdropping,etc.To maintain Data integrity,Confidentiality,prevent data loss,etc computer security is important issue to be maintained for it.A Data from computer can be hacked for not only harmful purposes but also for harmless purposes.There are many categories of Hackers which are divided according to different purposes or their functions to hack any data or websites.Computer security is important because some malicious mails,codes or different contents can destroy computer system.

THREATS,METHODS OF COMPUTER SECURITY &APPLICATION

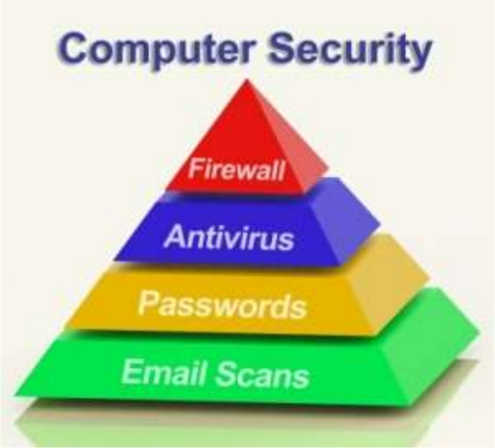


Fig.Computer Security

Computer security or cyber security is a mechanism to protect software or hardware as well as system database from unauthorized user or theft.
Some of the threats that can break computer security legally or illegally are

1. **IP Spoofing**
2. **Hacking**
3. **Eavesdropping**

1. **IP spoofing:** In this mechanism user creates IP that is Internet protocol packet along with IP address of source which will be hidden so that it cannot be identified. The attacker or spoofer hides the source machine address from this packets and views the different IP addresses which is expected by destination. The main use of IP spoofing is to create the jam condition for certain user machine whose address is shown to destination machine by attacker.

2. **Hacking:** It can be defined as acquiring an access to such system which is authorised by an individual and it is restricted to be accessed by public or unauthorised users. Nowadays everyone is carrying a threat in their mind whether their Email Ids ,Bank accounts or accounts and social sites are secured or not.

i. **Ethical Hacking:** It is legal type of hacking which is done for welfare of systems or user systems organizations. in this scheme only an authorized user can access the data of our system.

ii. **Non Ethical hacking:** It is illegal type of hacking. An individual who does such types of hacking are called as Black hat type of hackers. This type of hackers creates malware for the system which is hacked by them. They have complete control over an hacked system. It not only include computer system but also includes smart phones, Credit, Debit cards, tabs etc.It is also called as malicious hacking.

- **Hackers:** A person or user whose does the process of hacking is called hacker. There are many types of hackers

i. **White hat hackers**: This hackers hack the security for security purpose itself, Which are harmless to the systems. This hackers are mostly found in fields of such users who carry out penetration test and also vulnerability assessment. Online training and other requirements like certification are provided for this type of hacking that is ethical hacking

ii. **Black hat hackers**: they are also called crackers. These may prove more harmful or malicious to the system which system is hacked by black hat hackers. These hackers hack the system to access the information or perform some operations on it. These hackers can be individual or group of individual.

iii. **Grey Hat hackers**: This type of hackers play the role of both black as well as white hat hackers. although these hackers are not intentional hackers but still they are considered as illegal hackers.

iv. **Script Kiddie:** Script Kiddie itself has its meaning. Script means pre written coding or procedures and kiddie means A person who don’t have sufficient knowledge of hacking and dependent on different programmers or high level hackers.

3. **Eavesdropping:**Eavesdropping means listening or stealing information which is send by sender to intended destination without their permissions. In networking eavesdropping takes place in network layer of OSI reference model .This technique is mostly used by black hat hackers .This can be applied on only such data which not encrypted for security.This may lead to data loss or misuse of confidential data

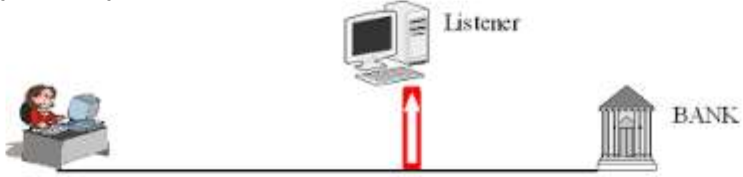


Fig.Eavesdropping

Some of the methods are developed to prevent computer and it’s data from hacking and other threats like spoofing too.

I. **Prevention from IP Spoofing:**

- Installation of Filtering Router.It doesn’t allow the interference of external network.Once the packet is sent by source it carries source IP address of Internal network and also it filter packets before sending.
- Installation of software called Antispam to prevent spoofing of Emails**.**

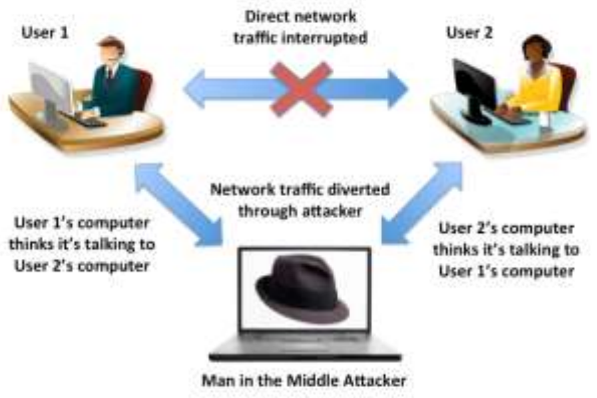
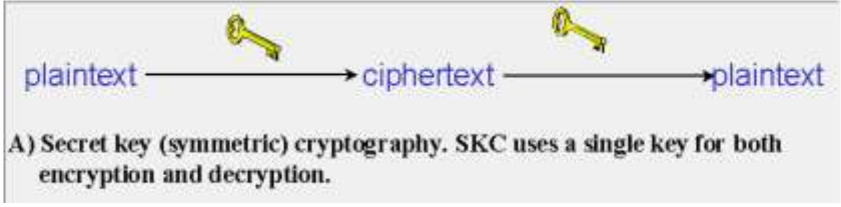

User 1
Direct network traffic interrupted
User 2
Network traffic diverted through attacker
User 1's computer thinks it's talking to User 2's computer
User 2's computer thinks it's talking to User 1's computer
Man in the Middle Attacker

Fig.Spoofing

II. **Cryptography:** It is a part of cryptology and cryptoanalysis.It uses microdots,covering the data by images & various methods to prevent data to get expose to other unauthorized users.It is a important field in computer security.The user who make the use of this cryptography are called cryptographers.Cryptography includes important points like maintaining confidentiality,dataintegrity,authenticating users i.e.sender and receiver .The data should be cryptographted in such a way that it cannot be identified by anyone.There should be no loss of data which is sent by source to destination.Whena information is sent from source to destination both should be able to authenticate each other to acknoweledge themselves that the data sent from source is received by excepted or intended destination There are various specified procedure or protocols for proper cryptography called a cryptosystem .they mostly include codes and mathematical codes. some of method are –

i. Secret key cryptography:

For both encrypting and decrypting only one key is required that is known as secret key cryptography.In this method the plaintext is sent by source but at first encrypted and the ciphertext is sent further to receiver .the same procedure is applied by receiver on ciphertext and decrypted to plaintext .All this procedure uses only one key and it is also known symmetric encryptions**.**



A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

Fig.Secret key Cryptography

ii. Public key cryptography:

In this two keys are involved one key is for fooling the other unauthorized users ,different destination which are trying to read the data from frames sent by source to intended destination,which is known as public key.And one key is encrypted for authorized destination or intended user ,Which is known as private key.This method is used to hide the actual data to prevent it from leaking to unintended user and kept it's confidentiality constant it is also called as asymmetric key algorithm.

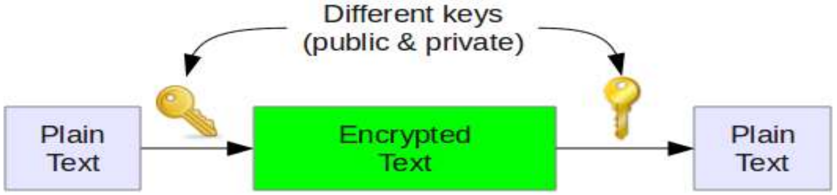


Fig.Public key Cryptography

Application:

1.**Commercial Transaction**:

It includes import/export-trading online transaction etc. this processes includes bodies like bank account, swapping of credit/debit cards to make transaction quickly. Huge payments are done online, this may give golden chance to hackers which may hack bank account numbers, credit/debit cards numbers and misuse it which gives rise to robbery. They can make the bank account empty in fraction of seconds.

2.**Industrial Fields**:

In industrial fields all the industrial equipments machines are handled by computers. It guides when and how the machine will work according to given command, if hackers make changes in this commands can cause a disaster in industries. This can be done by using IP Spoofing Technique.

3.**Devices:** Devices which are commonly used by individual like smart phones, tabs ,smart watches also can be hacked and the information gained from it can be misused. One can be tracked whose device has been hacked.

RESULTS AND DISCUSSION

To protect the computer from hacking and spoofing and other threats we can use some softwares like spyware,buster,antivirussoftware,firewalls,rootkillers,etc or hardwares or the combination of hardware and software.By using this kind of softwares we can provide a safeguard to our Computer and other computerized devices too.Some of the measures of computer security are-

1. Encryption of Harddisk drives.
2. Access should be limited
3. Portable storage devices used by user should be properly secured.
4. One should properly set the password for each account,websites,documents. To maintain it's confidentiality and secure it from spoofers and hackers.

CONCLUSION

The basic security architecture of legion system we have been presented.We have demonstrate that our design is flexible to accommodate a wide variety of security related mechanism.This flexibility is very difficult to successful deployment and use of metacomputing software.

ACKNOWLEDGEMENTS

We express our profound gratitude to our internal guide **Ms.Miss.Pawar M.R.** of Information Technology Department for his guidance and help through the development of this project work by providing us with required information with his guidance, co-operation and encouragementWe would like to thank **Mr.Phulawade.S.P.** Head of Department of Information Technology for his valuable guidance for bringing shape of this project.We express our special thanks to our principal **Prof.Gunjal Y.S.** on behalf of our Information Technology Department for his kind cooperation.

REFERENCES

[1] Author : Nick Lewis –Master of science in Information Assurance from Norwich University in 2015.
[2] Author:Garry Kessler-Cryptography
[3] http://csrc.nist.gov/
[4] http://www.aniltj.com/blog/2006/12/28/ThreatsToMessageExchangesInASOA.aspx
[5] http://etesis.nitrkl.ac.in/4868/1/109cs0435.pdf
[6] http://www.econsystems.com/5MP-USB-CAMERA-FAQ.asp

AUTHOR BIBLIOGRAPHY

	KulkarniPratiksha S. Information Technology Department, JCEI'S Jaihind Polytechnic Kuran, Tal – Junnar, Pune, India
	Jaid Swati D. Information Technology Department, JCEI'S Jaihind Polytechnic Kuran, Tal – Junnar, Pune, India
	NilakhAshwini B. Information Technology Department, JCEI'S Jaihind Polytechnic Kuran, Tal – Junnar, Pune, India