(UNIT-1)

INTRODUCTION

NEED FOR SECURING A NETWORK:

The network needs security against attackers and hackers. Network Security includes two basic securities. The first is the security of data information i.e. to protect the information from unauthorized access and loss. And the second is computer security i.e. to protect data and to thwart hackers. Here network security not only means security in a single network rather in any network or network of networks.
Now our need of network security has broken into two needs. One is the need of information security and other is the need of computer security.
On internet or any network of an organization, thousands of important information is exchanged daily. This information can be misused by attackers. The information security is needed for the following given reasons.

1. To protect the secret information users on the net only. No other person should see or access it.
2. To protect the information from unwanted editing, accidently or intentionally by unauthorized users.
3. To protect the information from loss and make it to be delivered to its destination properly.
4. To manage for acknowledgement of message received by any node in order to protect from denial by sender in specific situations. For example let a customer orders to purchase a few shares XYZ to the broader and denies for the order after two days as the rates go down.
5. To restrict a user to send some message to another user with name of a third one. For example a user X for his own interest makes a message containing some favourable instructions and sends it to user Y in such a manner that Y accepts the message as coming from Z, the manager of the organization.
6. To protect the message from unwanted delay in the transmission lines/route in order to deliver it to required destination in time, in case of urgency.
7. To protect the data from wandering the data packets or information packets in the network for infinitely long time and thus increasing congestion in the line in case destination machine fails to capture it because of some internal faults.

Another part of network security includes the computer security. Computer security means to protect your computer system from unwanted damages caused due to network. One of the major reason for such damages are the viruses and spywares that can wipe off all the information from your hard disk or sometimes they may be enough destructive and may cause hardware problems too. Certainly the network must be protected from such type of damaging software. The people who intentionally put such software on the network are called Hackers. As the network computers are part of it, so the computer security from Hackers is also a part of network security.
The needs of computer security from Hackers are as follows:-

> It should be protected from replicating and capturing viruses from infected files.

> It needs a proper protection from worms and bombs.

> There is a need of protection from Trojan Horses as they are enough dangerous for your computer.

PRINCIPLES OF SECURITY:

1. Confidentiality:

- Confidentiality is probably the most common aspect of information security. The principle of confidentiality specifies that only the sender and intended recipient should be able to access the contents of a message.

- Confidentiality gets compromised if an unauthorized person is able to access a message. Protection of confidential information is needed. An organization needs to guard against those malicious actions to endanger the confidentiality of its information.

- Example: Banking customers accounts need to be kept secret. Confidentiality not only applies to the storage of the information but also applies to the transmission of information. When we send a piece of the information to be stored in a remote computer or when we retrieve a piece of information from a remote computer we need to conceal it during transmission. Interception causes loss of message confidentiality.

2. Integrity:

- Information needs to be changed constantly. Integrity means that changes need to be done only by authorized entities and through authorized mechanisms. When the contents of a message are changed after the sender sends it, before it reaches the intended recipient it is said that integrity of the message is lost.

- Integrity violation is not necessarily the result of a malicious act; an interruption in the system such as a power surge may also create unwanted changes in some information.

- Modification causes loss of message integrity.

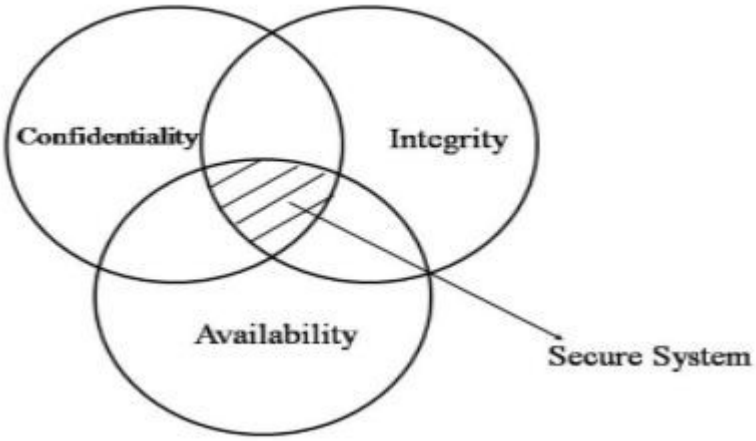
3. Availability:

- The principle of availability states that resources should be available to authorized parties at all times. The information created and stored by an organization needs to be available to authorized entities. Information is useless if it is not available.

- Information needs to be constantly changed which means it must be accessible to authorized entities. The unavailability of information is just as harmful for an organization as the lack of confidentiality or integrity.

- Example: The situation can be difficult for a bank if the customer could not access their accounts for transactions.

- Interruption puts the availability of resources in danger.



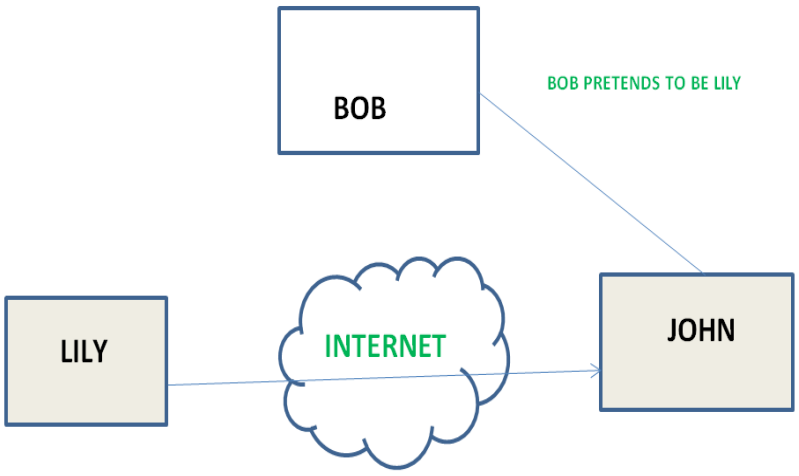
- The diagram above explains the balance concept. The right balance of the three goals is needed to build a secure system. If the goals are not balanced then a small hole is created for attackers to nullify the other objectives of security. Having a highly confidential system but low availability then the system is not secure.

- Example: A system can protect confidentiality and integrity but if the resource us not available the other two goals also are of no use.

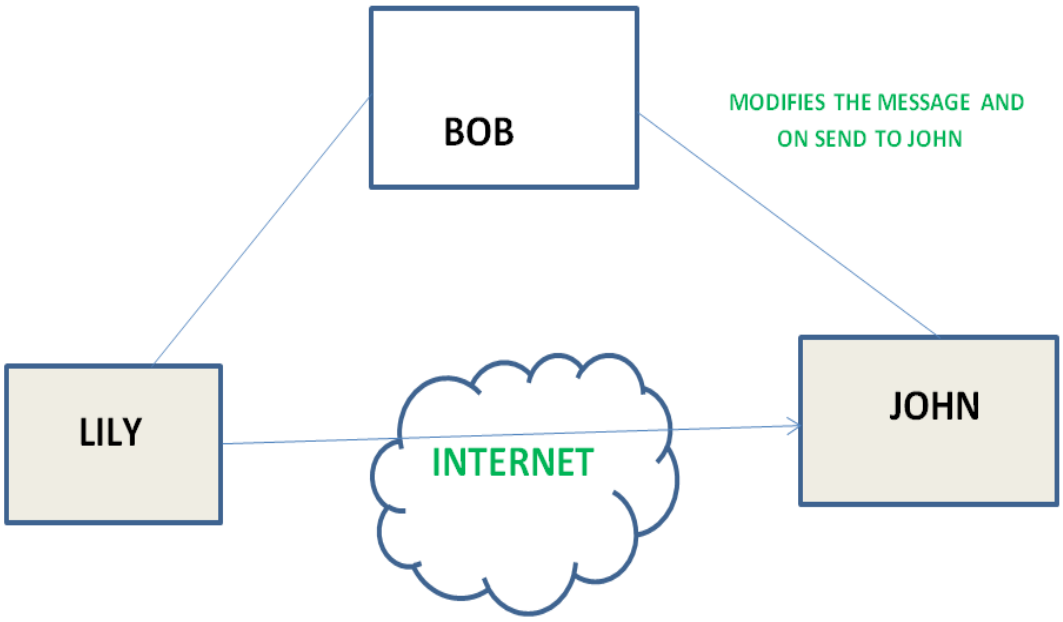
TYPES OF ATTACKS:

Active attacks: An Active attack attempts to alter system resources or effect their operations. Active attack involve some modification of the data stream or creation of false statement. Types of active attacks are as following:

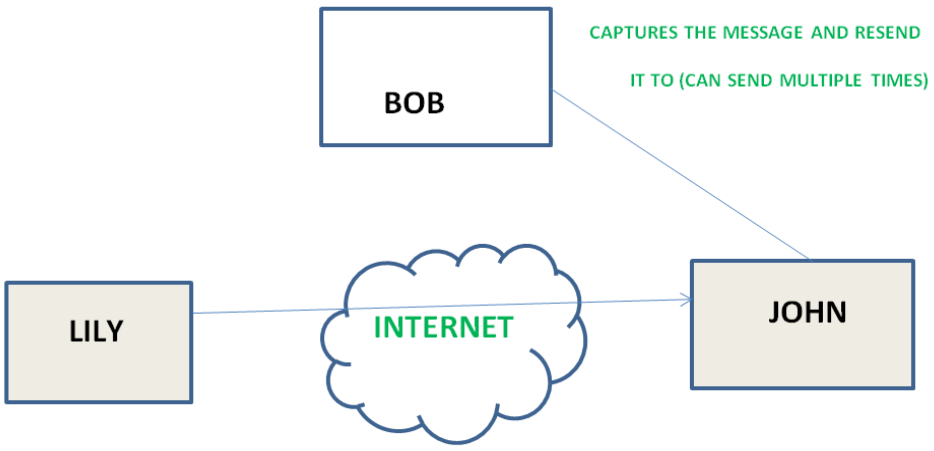
1. **Masquerade** – Masquerade attack takes place when one entity pretends to be different entity. A Masquerade attack involves one of the other form of active attacks.



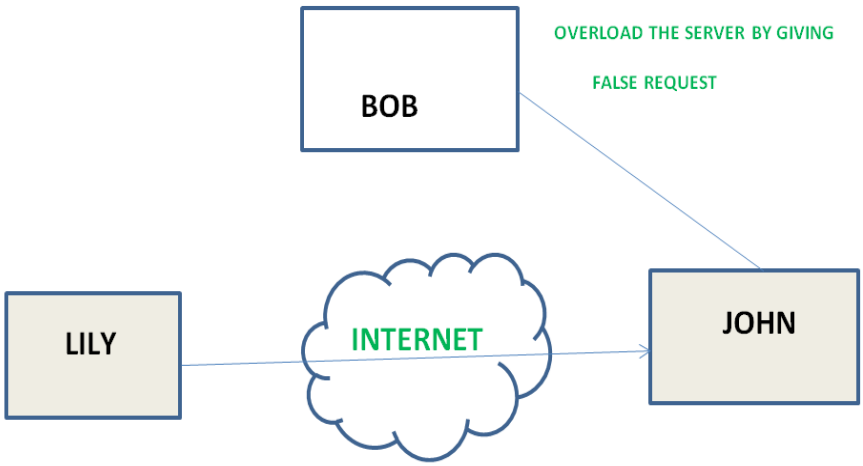
2. **Modification of messages** – It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorised effect. For example, a message meaning "Allow JOHN to read confidential file X" is modified as "Allow Smith to read confidential file X".



1. **Repudiation** – This attack is done by either sender or receiver. The sender or receiver can deny later that he/she has send or receive a message. For example, customer ask his Bank "To transfer an amount to someone" and later on the sender(customer) deny that he had made such a request. This is repudiation.
2. **Replay** – It involves the passive capture of a message and its subsequent the transmission to produce an authorized effect.

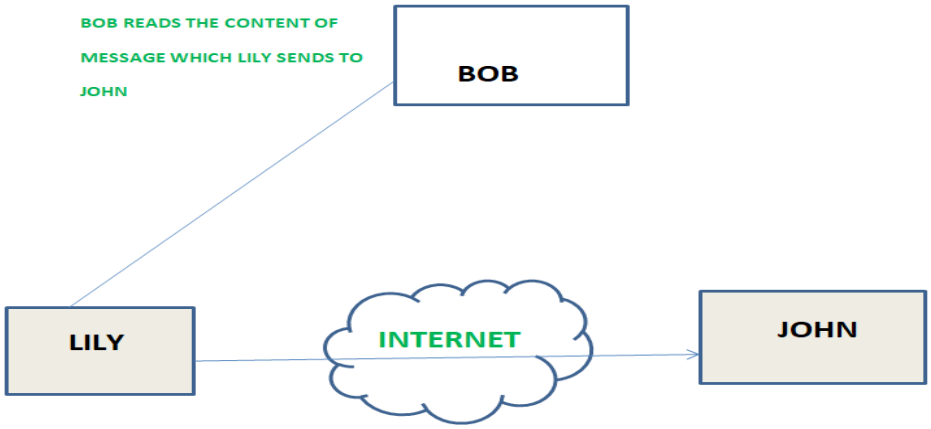


3. **Denial of Service** – It prevents normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network wither by disabling the network or by overloading it by messages so as to degrade performance.

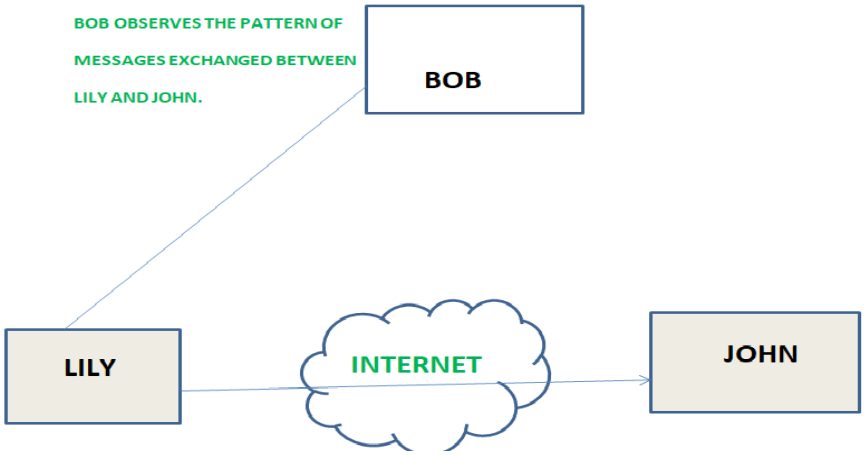


Passive attacks: A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information is being transmitted. Types of Passive attacks are as following:

1. **The release of message content** – Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.



2. **Traffic analysis** – Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message. The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.



INTRODUCTION TO CYBER CRIME:

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers.

Cybercrime may also be referred to as computer crime.

Common types of cybercrime include online bank information theft, identity theft, online predatory crimes and unauthorized computer access. More serious crimes like cyberterrorism are also of significant concern.

Cybercrime encompasses a wide range of activities, but these can generally be broken into two categories:

- Crimes that target computer networks or devices. These types of crimes include viruses and denial-of-service (DoS) attacks.
- Crimes that use computer networks to advance other criminal activities. These types of crimes include cyberstalking, phishing and fraud or identity theft.

The FBI identifies cybercrime fugitives who have allegedly committed bank fraud and trafficked counterfeit devices that access personal electronic information. The FBI also provides information on how to report cybercrimes, as well as useful intelligence information about the latest cybercriminals.

CYBER LAW INDIAN PRESPECTIVE

In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000.

This Act aims to provide the legal infrastructure for e-commerce in India. And the cyber laws have a major impact for e-businesses and the new economy in India. So, it is important to understand what are the various perspectives of the IT Act, 2000 and what it offers.

The Information Technology Act, 2000 also aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability. Some highlights of the Act are listed below:

Chapter-II of the Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify an electronic record by use of a public key of the subscriber.

Chapter-III of the Act details about Electronic Governance and provides inter alia amongst others that where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is -
rendered or made available in an electronic form; and accessible so as to be usable for a subsequent reference.

The said chapter also details the legal recognition of Digital Signatures.

Chapter-IV of the said Act gives a scheme for Regulation of Certifying Authorities. The Act envisages a Controller of Certifying Authorities who shall perform the function of exercising supervision over the activities of the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities as also specifying the various forms and content of Digital Signature Certificates. The Act recognizes the need for recognizing foreign Certifying Authorities and it further details the various provisions for the issue of license to issue Digital Signature Certificates.

Chapter-VII of the Act details about the scheme of things relating to Digital Signature Certificates. The duties of subscribers are also enshrined in the said Act.

Chapter-IX of the said Act talks about penalties and adjudication for various offences. The penalties for damage to computer, computer systems etc. has been fixed as damages by way of compensation not exceeding Rs. 1,00,00,000 to affected persons. The Act talks of appointment of any officers not below the rank of a Director to the Government of India or an equivalent officer of state government as an Adjudicating Officer who shall adjudicate whether any person has made a contravention of any of the provisions of the said Act or rules framed there under. The said Adjudicating Officer has been given the powers of a Civil Court.

Chapter-X of the Act talks of the establishment of the Cyber Regulations Appellate Tribunal, which shall be an appellate body where appeals against the orders passed by the Adjudicating Officers, shall be preferred.

Chapter-XI of the Act talks about various offences and the said offences shall be investigated only by a Police Officer not below the rank of the Deputy Superintendent of Police. These offences include tampering with computer source documents, publishing of information, which is obscene in electronic form, and hacking.

The Act also provides for the constitution of the Cyber Regulations Advisory Committee, which shall advice the government as regards any rules, or for any other purpose connected with the said act. The said Act also proposes to amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them in tune with the provisions of the IT Act.

Advantages of Cyber Laws

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.

In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature.

From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.

Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.

Digital signatures have been given legal validity and sanction in the Act.

The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.

The Act now allows Government to issue notification on the web thus heralding e-governance.

The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.

The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.

Under the IT Act, 2000, it shall now be possible for corporates to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore.

CYBER ETHICS

Cyber ethics is the study of ethics pertaining to computers, covering user behavior and what computers are programmed to do, and how this affects individuals and society. For years, various governments have enacted regulations while organizations have explained policies about cyber ethics.

With the increase of young children using the internet, it is now very essential than ever to tell children about how to properly operate the internet and its dangers. It is especially hard to talk to teens because they do not want to be lectured about what is right and wrong. They seem to think they have it all sorts out. That is why is it

is important to instill appropriate cyber etiquette at an early age but if you haven't there is still time to tell to your child.

Responsible Behaviors on the Internet

Cyber ethics concerns to the code of responsible behavior on the Internet. Just as we are taught to act responsibly in everyday life. The responsible behavior on the internet in many ways aligns with all the right behavior in everyday life, but the results can be significantly different.

Some people try to hide behind a false sense of obscurity on the internet, believing that it does not matter if they behave badly online because no one knows who they are or how to search them. That is not all the time true; browsers, computers and internet service providers may keep logs of their activities which can be used to spot illegal or inappropriate behavior.

The Government has taken a positive role in making resources for parents and children to learn about cyber ethics. This is a growing problem and without parents and teachers using the resources available nothing can be done to prepare future generations of internet users from being safe online.

Following some issues are increasing daily due to children using the internet improperly and we have to take care of it.

Copyrighting or Downloading

Copyright or downloading is a major issue because children don't know copyright policies. They only try to search what they need from the web and download it for their purpose. Their thinking is like "if everybody is doing it therefore it's ok", but an understandable and an age appropriate lesson on Cyber Ethics could help children to learn the risks involved in Internet downloading.

Crime and Punishment

Children do not believe that they will get into any real problem from neglecting the use of cyber ethics. It has become easy to track the origin of wrong activity over the internet to an individual user. There is not much anonymity as a child may trust. The United States Department of Justice has a recent list of Federal Computer Crime Cases teens this is a best way to show children the costly consequences of their internet actions.

Internet Hacking

Hacking done by stealing classified information, stealing passwords to get into a site and also recasting a website without permission. Since the world is run on computers it is important that hackers are stopped. They could create viruses that could shut down important websites or computer systems. So we have to make our children aware by telling its importance.

Cyberbullying

Cyberbullying is increasing and people are becoming aware of its effects on children. Cyberbullying is bullying that takes place carrying electronic technology. Electronic technology carried by devices and equipment such as cell phones, computers, and tablets as well as communication tools including social media sites, text messages, website and chat.

When a child encounters cyber bullying that they should:

- Tell a trusted adult, and keep telling them until they take action.
- Avoid to open, read or respond to messages from cyber bullies.
- Always keep messages from bullies. They may be needed to take corrective action
- Use software to block bullies if they encounter them through chat or IM.

Use of technology by students is globally accepted as it facilitates the searching and retrieval of information needed for their academics and consequently the successful completion of their education programs. They need to be aware and knowledgeable about the ethics surrounding the use of ICT is therefore, important. Students must be aware and possess the knowledge about cyber ethics. Therefore, cyber ethics education must be provided to students by the school and colleges.

ETHICAL HACKING

Ethical hacking

Hacking is quite useful in the following scenarios:

To recover lost information, especially in case you lost your password.To perform penetration testing to strengthen comput
er and network security.
To put adequate preventative measures in place to prevent security breaches. To have a computer system that prevents malicious hackers from gaining access.
Disadvantages of Hacking

Hacking is quite dangerous if it is done with harmful intent. It can cause:
Massive security breach.Unauthorized system access on private information.Privacy violation.Hampering system operation.Denial of service attacksMalicious attack on the system.
Purpose of Hacking

There could be various positive and negative intentions behind performing hacking

activities. Here is a list of some probable reasons why people indulge in hackingactivities:
Just for funShow-offSteal important informationDamaging the systemHampering priv
acy
Money extortionSystem security testingTo break policy compliance
Ethical hacking

2.

Ethical Hacking – Hacker Types

Hackers can be classified into different categories such as white hat, black hat, andgrey

hat, based on their intent of hacking a system. These different terms come from old

Spaghetti Westerns, where the bad guy wears a black cowboy hat and the good guywears

a white hat.

White Hat Hackers

White Hat hackers are also known as
Ethical Hackers
. They never intent to harm a

system, rather they try to find out weaknesses in a computer or a network system as a

part of penetration testing and vulnerability assessments.

Ethical hacking is not illegal and it is one of the demanding jobs available in the ITindustry.

There are numerous companies that hire ethical hackers for penetration testing and

vulnerability assessments.

Black Hat Hackers

Black Hat hackers, also known as
crackers
, are those who hack in order to gain

unauthorized access to a system and harm its operations or steal sensitive information.

Black Hat hacking is always illegal because of its bad intent which includes stealing

corporate data, violating privacy, damaging the system, blocking networkcommunication,

etc.

Grey Hat Hackers

Grey hat hackers are a blend of both black hat and white hat hackers. They act without

malicious intent but for their fun, they exploit a security weakness in a computersystem

or network without the owner's permission or knowledge.

Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access.
Example of Hacking: Using password cracking algorithm to gain access to a system

Computers have become mandatory to run a successful businesses. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. Hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cyber crimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.

In this tutorial, we will learn-

- What is Cyber Crime?
- Types of Cyber Crime
- What is Ethical Hacking?
- Why Ethical Hacking?
- Legality of Ethical Hacking
- Summary

Before we go any further, let's look at some of the most commonly used terminologies in the world of hacking.

Who is a Hacker? Types of Hackers

A **Hacker** is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.

Hackers are classified according to the intent of their actions. The following list classifies hackers according to their intent.

Symbol	Description
	**Ethical Hacker (White hat):** A hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetrationTesting and vulnerability assessments.

	**Cracker (Black hat):** A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.
	**Grey hat:** A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.

	**Script kiddies:** A non-skilled person who gains access to computer systems using already made tools.
	**Hacktivist:** A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website.
	**Phreaker:** A hacker who identifies and exploits weaknesses in telephones instead of computers.

What is Cybercrime?

Cyber crime is the use of computers and networks to perform illegal activities such as spreading computer viruses, online bullying, performing unauthorized electronic fund transfers, etc. Most cybercrimes are committed through the internet. Some cybercrimes can also be carried out using Mobile phones via SMS and online chatting applications.

Type of Cybercrime

- The following list presents the common types of cybercrimes:

- **Computer Fraud:** Intentional deception for personal gain via the use of computer systems.
- **Privacy violation:** Exposing personal information such as email addresses, phone number, account details, etc. on social media, websites, etc.
- **Identity Theft:** Stealing personal information from somebody and impersonating that person.
- **Sharing copyrighted files/information:** This involves distributing copyright protected files such as eBooks and computer programs etc.
- **Electronic funds transfer:** This involves gaining an un-authorized access to bank computer networks and making illegal fund transfers.
- **Electronic money laundering:** This involves the use of the computer to launder money.
- **ATM Fraud:** This involves intercepting ATM card details such as account number and PIN numbers. These details are then used to withdraw funds from the intercepted accounts.
- **Denial of Service Attacks:** This involves the use of computers in multiple locations to attack servers with a view of shutting them down.
- **Spam:** Sending unauthorized emails. These emails usually contain advertisements.

What is Ethical Hacking?

Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses. Ethical hackers must abide by the following rules.

- Get **written permission** from the owner of the computer system and/or computer network before hacking.
- **Protect the privacy of the organization** been hacked.
- **Transparently report** all the identified weaknesses in the computer system to the organization.
- **Inform** hardware and software vendors of the **identified weaknesses**.

Why Ethical Hacking?

- Information is one of the most valuable assets of an organization. Keeping information secure can protect an organization's image and save an organization a lot of money.
- Hacking can lead to loss of business for organizations that deal in finance such as PayPal. Ethical hacking puts them a step ahead of the cyber criminals who would otherwise lead to loss of business.

Legality of Ethical Hacking

Ethical Hacking is legal if the hacker abides by the rules stipulated in the above section on the definition of ethical hacking. The International Council of E-Commerce Consultants (EC-Council)provides a certification program that tests individual's skills. Those who pass the examination are awarded with certificates. The certificates are supposed to be renewed after some time.

Summary

- Hacking is identifying and exploiting weaknesses in computer systems and/or computer networks.
- Cybercrime is committing a crime with the aid of computers and information technology infrastructure.
- Ethical Hacking is about improving the security of computer systems and/or computer networks.
- Ethical Hacking is legal.

ATTACKER

An **attack** is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset." Thus, an **attacker** is the individual or organization performing these malicious activities.

An attacker may be a disgruntled insider that deletes sensitive files or disrupts the business by any means to achieve their goals.

PHREAKER

A phreak is someone who breaks into the telephone network illegally, typically to make free long-distance phone calls or to tap phone lines. The term is now sometimes used to include anyone who breaks or tries to break the security of any network. Recently, the phone companies have introduced new security safeguards, making phreaking more difficult.

phreaking was originally a more innocent occupation and hackers would sometimes take up the challenge. The typical phreak was or is usually equipped with a specially-made "box" designed to "fool" the network in some way. Different boxes, somehow named for different colors but not necessarily painted any color, are used for different phreak approaches. A "black box" allows you to make free calls from a home phone; a red box" to make free calls on a pay phone; and the infamous "blue box" provides complete control over the telephone system. If you look hard enough on the Web, you'll probably find directions on how to make all of these boxes. (But note that using the boxes as directed is probably illegal and any directions you find may be out-of-date.)

A brief analysis for Pretty Good Privacy

ABSTRACT

The goal of this paper is to demonstrate how the Pretty Good Privacy works from theoretical aspects and to investigate the reliability of Pretty Good Privacy in practical ways. Some important algorithms will be discussed, including Hash function, DES, RSA, MD5. Then, attacks aiming Pretty Good Privacy implementing will be displayed, in order to proof whether it has durable reliability.

1. INTRODUCTION

As the Internet technology and applications are becoming much more accessible than ever before, the population using the Internet has been growing exponentially these years. Because of none set-up costs for Email using and Email's asynchrony (in other words, people connecting each other do not bother to exchange messages in the arranged time), Email has become one of the most quick, convenient, and economical communication styles. Meanwhile, the security issues about Email are getting obvious. In fact, the delivery process of Email messages is repeated on the network replication procedure. Consequently, it is easy for unauthorized people to theft, tamper, or even damage Email messages, in terms of the uncertainty of network transmissions.

Therefore, there is an urgent need for public users to encrypt messages and ensure the security of transmission through the

Internet.

Under this circumstance, PGP (Pretty Good Privacy)[1] has emerged. Pretty Good Privacy is a program that uses encryption to protect the privacy of your electronic mail and the files that you store on your computer (Garfinkel, 1995)[2]. It was firstly invented and published to the Internet by Philip Zimmermann in 1991. PGP itself is not an encryption algorithm, but a completed security program package integrating some of the encryption algorithm, for instance, RSA, IDEA, AES, etc (Harold F. Tipton, 2008). Philip Zimmermann has completed the following main jobs: 1. choosing some excellent algorithms as basic components for the encryption algorithm, then put them together into an application program; 2. making a program package including important files, later turning it to open-sources; 3. co-operating with enterprises in order to occupy the markets. (Mollin, 2006)

This paper is constructed as follows. In section two we indicate how dose PGP works. In section three we briefly survey the reliability from practical angle.

2. THE PRINCIPLE OF IMPLEMENTING PGP

As we have known, PGP is not only the name of program, but also the name of a network standard (RFC 2440: Open PGP Message Format (J. Callas, 1998)). In this section, we mainly discuss the PGP as RFC standard.

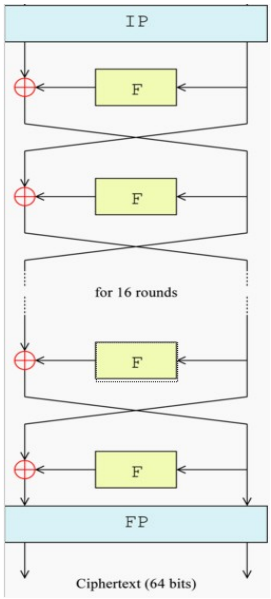
---

[1] PGP and Pretty Good Privacy are trademarks of Philip Zimmermann.
[2] Notice that this definition is not the only one, but a common idea among the academic realms.

PGP is a kind of system to protect the privacy of electronic documents based on 4 sections, namely, data compression, hashing, symmetric-cryptography, and public-key cryptography, each of which includes their own cryptographic algorithms, i.e. Hash function, DES (Data Encryption Standard), RSA, MD5. We will focus on how these algorithm works.

2.1 HASH FUNCTION

A hash function H is a computation which puts a variable-size input into the function and returns a fixed-size output, which is called the hash value (Thomas H. Cormen, 2001). The value is usually called message digest or digest (i.e. hashing a 3M file, outputting a 128 bit digest). Message digest represents the characteristics of the original data. When the original data changes, the re-generated message digest will also change, even if the change is only a very small part of the original data. Hence, hash function can be sensitive to detect whether the original data has been tampered. Combined with other algorithms, hash function can be used to protect the integrity of original data. Classic hash functions include: MD5, SHA-1, HMAC, GOST, etc.



What makes a good one-way[3] hash function?

1. The unfeasibility of reverse computing. Take arbitrary M and H,

[3] "One-way" in the name refers to the property of such functions: they are easy to compute, but their reverse functions are very difficult to compute.

h=H(m) can be computed easily, but it is not the case vice versa.

2. Weak collision property. Take arbitrary M, to find another M' satisfying H(M')=H(M) is unfeasible.

3. Strong collision property. To find a pair (M, M') satisfying H(M')=H(M) is unfeasible (Thomas H. Cormen, 2001).

2.2 DES (Data Encryption Standard)

DES is a kind of symmetric cryptography, which means the same key will be used in both encryption and decryption process. Its blocks and keys have a size 64-bits and 56-bits Figure 1 respectively. DES was developed by IBM, and adopted by National Bureau of Standard and American National Standard Institute in 1976. The overall Feistel structure of DES was displayed by Figure 1 (WIKIPEDIA, 2009).

The encryption steps are given as follows:

- Input is a plaintext block of the size 2w bits;
- The block is divided into two parts L and R;
- Two parts going through n rounds of processing;
- At every round, a function F (round function) is applied to the right half using a (sub)key, the result is XOR'cd with the left half of the data;
- At every round a new (sub) key may be used; all (sub) keys are generated from the same secret key (Lisitsa, 2008).

2.3 RSA

In 1978, Ron Rivest, Adi Shamir, and Leonard Adleman who were

at MIT issued the RSA algorithm to the public. The word “RSA” is the combination of their family name’ initials (Robinson, 2003). RSA is an asymmetric algorithm, which generally means two kinds of different keys are used in the processes of encryption and decryption, namely, public key and private key. Taking a metaphor, public keys, private keys and money are similar to a person’s bank account numbers, PINs, messages respectively. The account number can be known by everyone hence other people could be able to transmit the money to his/her account. However, no one consider it normal to tell the PIN to somebody else, or else his/her money in the bank will not be safe anymore. Furthermore, RSA algorithm is the one that can combine encryption and digital signature. Because of its durability, safety, simplicity, it has been accepted by the public as one of the most excellent public key encryption algorithms.

The generation of RSA keys

- The algorithm picks up two random and large primes p and q, then computes: $n = p * q$ and $\varphi(n) = (p-1) * (q-1)$.
- Uses the random encryption key e satisfying $1 < e < n$ and $\gcd(e, \varphi(n)) = 1$.
- Computes the unique $d \in N$, $ed \equiv 1 \pmod{\varphi(n)}$.
- Issues (n, e) as public keys, while keeps d, p, q, and$\varphi(n)$ as private keys (Mollin, RSA and public-key cryptography, 2003).

2.4 MD5

As an evolutionary version of MD4, MD5 (Message Digest algorithm 5) was published by Ron Rivest in early 90s. Actually, MD5 also

belongs to the hash algorithm, as what we have discussed above. Therefore, we will not bother to explain the principle of this algorithm. But one thing still need attention: although reports about decryption of MD5, HAVAL-18, MD4, and RIPEMD have been made by Xiaoyun Wang at Shandong University, in Crypto'2004, it is too haste to draw a conclusion that those algorithms all have been decrypted. In fact, Wang's decryption method just raised the decrypting efficiency to SHA-1 by 2000 times. It is not a big threaten to SHA-1, but till, it puts the SHA-1 to the surviving edge. No need to worry, we still have SHA-256 and SHA-512 to use. At the same time, experts are working hard on developing new hash functions.

3. THE RELIABILITY OF PGP

Using protection program does not guarantee a 100% security. Even if someone put the most secure lock on the door, the thief can still come into his/her house by the window. That is to say, a computer equipped with PGP can still be attack easily. There are a lot of attacks aiming to PGP, here we will only study some of these attacks.

Forms of attacks:

1. Attacking public and private Keys by Brute-Force is the most direct attack to PGP. In this case, the security of PGP depends on that of RSA and IDEA using by PGP. Hackers try to decrypt the key of PGP used for encryption.
2. The security of private keys of PGP is based on the following two points: accessing the private key and the degree of knowing about passwords of every private key. To use the private key, two points we've mentioned above is needed, accordingly, so dose attacks to private keys.

3. Since public keys depended by PGP play a crucial rule in the whole process, a lot of hackers will focus on attacking public keys.

When it comes to private keys, vulnerabilities of PGP's private keys can be investigated through the following steps. "In a chosen cipher-text attack, a hacker creates a message and then sends it to a targeted user with the expectation that this user will send the message to other users. When the targeted user distributes the message in an encrypted form, the hacker listens to the messages and computes the key from the newly created cipher-text[4]" (Michael Cross, 2002).

Then, our discussion will focus on the attacks of the public key.
According to the procedure of implementing PGP, let us consider a simple case first. Hacker C intercepts public keys of A and B when they are exchanged by their owner. Next, C uses his/her own public key to replace that of both A and B. In other words, both A and B will consider C's public key as each other's public key. Finally, C can listen the messages between A and by using his/her private key.

The above procedure is based on A and B passing public keys to each other and C intercepting the public keys. However, it is clear that if A and B use the certificated signature when they exchange their public keys, they can avoid the above-mentioned attacks effectively, for the reason that C can not pose his/her public key to A or B since they will ask their common authorized user D for each other's public key, thence increasing the difficulty of attacking. Unfortunately, Hackers still have some ways to attack.

[4] This is cited from page 131 [Michael Cross, 2002].

1. The public key ring will be checked only after it has been changed. That is to say, if new keys or signatures come, PGP will check them and put a tag on them indicating they have been checked, then PGP will never check them again. Therefore, hackers can modify the signatures in a public key ring to an “already-checked” one. By this procedure, the system will not check these changed signatures and hackers can attack again.
2. Another attack to a PGP public ring is possible though the use of PGP. Every public key have a “valid bit” included in the prefix form. PGP will compute the length of new arrived signature’s valid bit, and then put it into the buffer of the public key ring. Hackers could modify this valid bit from public key ring, thence making users trust this invalid key. For example, user A will check whether the public key received is valid in order to set the value to it. Meanwhile, the hacker C could make this key valid by changing its valid bit, thereby letting A believe that what A has received is really belonged to B, although there is no signature to identify the validity of this public key, regardless of the fact that, in fact, that is C’s public key.
3. The inducer’s trust key exists in the buffer of public key ring. The trust key can define the amount/size of trust to it. Therefore, PGP will accept an invalid key as a valid key by using a key with certain trust value to give a signature to that invalid key. For instance, if A/B totally trust certificate PK_D coming from D, then both A and B have the public key of D. But if a hacker C changed PK_D to PK_c, then C could use PK_c to signage for other public keys, hence making A/B trust those changed public keys (Vlastimil Klíma, 2001).

4. CONCLUSION

This paper represents the achievable theory of PGP from the algorithms of hash, DES, RSA and MD5. Some secure issues, including attack forms, are also described in the essay.
From what we have discussed above, we can safely conclude that one of the most serious problems within the PGP procedure should be that public key ring is no protection procedure providing safety for buffers. Everyone could be able to modify any bit of the public key ring without being found though any binary-file tools who can understand PGP codes and who access public key ring. According to this, PGP program should protect public key ring carefully, and detect any malice tamper immediately.

The PGP algorithm has never been proofed as having 100% security. Even though the mathematics on which PGP are based are considered very safe, but it is feasible to attack PGP as long as hackers have found some bugs of it. In other words, nothing has exact safety. If there is enough time and sources, every encryption algorithm will be conquered. However, the question is whether it is worthwhile to decode the data protected by encryption algorithms by spending certain amount of time and sources. We should be aware the fact that, the cost of decryption has been cutting as the time passes, because computers are becoming more and more efficient, and the hardware getting more and more chip. Anyway, hackers still have a long way to go in order to exceed the cryptologists.

REFERENCES

1. Garfinkel, S. (1995). *PGP: Pretty Good Privacy.* O'Reilly Media, Inc.
2. Harold F. Tipton, M. K. (2008). *Information Security Management Handbook.* AUERBACH.
3. J. Callas, L. D. (1998, 11). *OpenPGP Message Format.* Retrieved 10 25, 2009, from The Internet Engineering Task Force : http://www.ietf.org/rfc/rfc2440.txt
4. LisitsaAlexei. (2008, 12, 12). accessing date: 10, 21, 2009 source: University of Liverpool: http://www.csc.liv.ac.uk/~alexei/COMP522/COMP522-SymmetricEnc-07.pdf
5. Michael Cross, N. L. (2002). *Security plus study guide and DVD training system* (1th edition ed.). Syngress.
6. Mollin, R. A. (2006). *An introduction to cryptography* (2th edition ed.). Chapman & Hall/CRC.
7. MollinA.Richard. (2003). RSA and public-key cryptography. CHAPMAN & HALL/CRC.
8. RobinsonSara. (2003). Still Guarding Secrets after Years of Attacks, RSA Earns Accolades for its Founders. SIAM News, 36.
9. Thomas H. Cormen, C. E. (2001). *Introduction to Algorithms* (2nd edition ed.). The MIT Press.
10. Vlastimil Klíma, a. T. (2001, Mar). Attack on Private Signature Keys of the OpenPGP format, PGPTM programs and other applications compatible with OpenPGP. *Citeseer* .
11. *WIKIPEDIA.* (2009, 10, 21). Retrieved 10 25, 2009, from http://en.wikipedia.org/wiki/Symmetric-key_cryptography
12. WIKIPEDIA. (2009, 10, 23). Retrieved 10, 25, 2009, from http://en.wikipedia.org/wiki/Data_Encryption_Standard#The_Feistal_.28F.29_function