ISSN:0975-9646

Poornachander V / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (3) , 2016, 1648-1654

Security Issues on Cryptography and Network Security

Poornachander V[#]

[#]*M.Sc, M.Tech (CSE), Department of Computer Science, Government Degree & P.G. College Narsampet,Warangal, Telangana, INDIA*

***Abstract*— This paper deals with some security issues which are occurred often in some areas like personal systems, Networking in Industries etc. Here we discussed some concepts which are related to encryption techniques in Cryptography like Security attacks, Services and Mechanism, Cryptanalysis, Steganography, Cryptographic attacks, Symmetric and public key algorithm, Conventional, Classical and Transposition techniques. And there is some network security related threats along with their solutions like non-complex, weak network access passwords, viruses and worms, Trojen Horses, SPAM, Phising, Packet sniffers, Shared computers, Zombie computers and botnets.**

***Index Terms*—Cryptography, Encryption Techniques, Network Security, Security Threats and solutions.**

I. INTRODUCTION

Computer data often travels from one computer to another, leaving the safety of its protected physical surroundings. Once the data is out of hand, people with bad intention could modify or forge our data, either for amusement or for their own benefit. Cryptography can reformat and transform our data, making it safer on its trip between computers. The technology is based on the essentials of secret codes, augmented by modern mathematics that protects our data in powerful ways. • Computer Security - generic name for the collection of tools designed to protect data and to thwart hackers • Network Security - measures to protect data during their transmission • Internet Security - measures to protect data during their transmission over a collection of interconnected networks

A. SECURITY ATTACKS, SERVICES AND MECHANISMS

To assess the security needs of an organization effectively, the manager responsible for security needs some systematic way of defining the requirements for security and characterization of approached to satisfy those requirements. One approach is to consider the following three aspects of information security.

Security Attack: Any action that compromises the security of information owned by an organization.

Security mechanism: A mechanism that is designed to detect, prevent or recover from a security attack.

Security Service: A Service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks and they make use of one or more security mechanisms to provide the service.

II. CRYPTOGRAPHY–

Cryptographic systems are generally classified along three dimensions:

1.Type of operations used for transforming plain text to cipher text: All the encryption algorithms are based on two general principles: ***Substitution,*** in which each element in the plaintext is mapped into another element, and ***Transposition,*** in which elements in the plain text are rearranged.

2. The Number of Keys used :

If the sender and receiver uses same key then it is said to be ***Symmetric key (or) Single Key (or) Conventiontional encryption.***

If the sender and receiver use different keys then it is said to be ***Public Key encryption.***

3. The way in which the plain text is processed:

A block cipher processes the input and block of elements at a time, producing output block for each input block.

A Stream cipher processes the input elements continuously, producing output element one at a time, as it goes along.

III. CRYPTANALYSIS:

The process of attempting to discover X or K or both is known as cryptanalysis. The strategy used by the cryptanalysis depends on the nature of the encryption scheme and the information available to the cryptanalyst. There are various types of cryptanalytic attacks based on the amount of information known to the cryptanalyst.

1. Cipher text only – A copy of cipher text alone is known to the cryptanalyst.

2. Known plaintext – The cryptanalyst has a copy of the cipher text and the corresponding plaintext.

3. Chosen plaintext – The cryptanalysts gains temporary access to the encryption machine. They cannot open it to find the key, however; they can encrypt a large number of suitably chosen plaintexts and try to use the resulting cipher texts to deduce the key.

4. Chosen cipher text – The cryptanalyst obtains temporary access to the decryption machine, uses it to decrypt several string of symbols, and tries to use the results to deduce the key.

IV. STEGANOGRAPHY-

A plaintext message may be hidden in any one of the two ways. The methods of steganography conceal the existence of the message, whereas the methods of cryptography render

the message unintelligible to outsiders by various transformations of the text.

A simple form of steganography, that is time consuming to construct is one in which an arrangement of words or letters within an apparently innocuous text spells out the real message.

e.g.,a. The sequence of first letters of each word of the overall message spells out the real (Hidden) message.

b. Subset of the words of the overall message is used to convey the hidden message.

Various other techniques have been used historically, some of them are

a. Character marking – selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held to an angle to bright light.

b. Invisible ink – a number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.

c. Pin punctures – small pin punctures on selected letters are ordinarily not visible unless the paper is held in front of the light.

d. Typewritten correction ribbon – used between the lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.

Drawbacks of steganography is requires a lot of overhead to hide a relatively few bits of information. Once the system is discovered, it becomes virtually worthless.

V. SECURITY SERVICES-

The classification of security services are as follows:

Confidentiality: Ensures that the information in a computer system a n d transmitted information are accessible only for reading by authorized parties. E.g. Printing, displaying and other forms of disclosure.

Authentication: Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.

Integrity: Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.

Non repudiation: Requires that neither the sender nor the receiver of a message be able to deny the transmission.

Access control: Requires that access to information resources may be controlled by or the target system.

Availability: Requires that computer system assets be available to authorized parties when needed.

VI. SECURITY MECHANISMS -

One of the most specific security mechanisms in use is cryptographic techniques. ***Encryption or encryption***-like transformations of information are the most common means of providing security.

Some of the mechanisms are 1 Encipherment 2 Digital Signature 3 Access Control.

VII. SECURITY ATTACKS -

There are four general categories of attack which are listed below.

1.***Interruption:*** An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability.

e.g., Destruction of piece of hardware, cutting of a communication line or Disabling of file management system. 2.***Interception***: An unauthorized party gains access to an asset. This is an attack on confidentiality. Unauthorized party could be a person, a program or a computer.

e.g., wire tapping to capture data in the network, illicit copying of files.

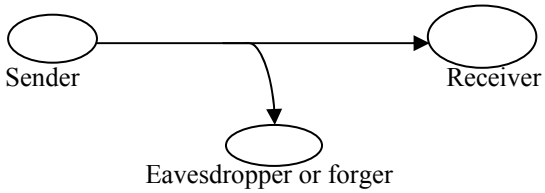
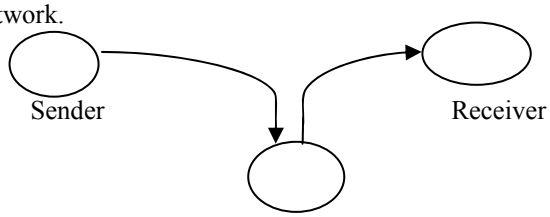


fig 4.1

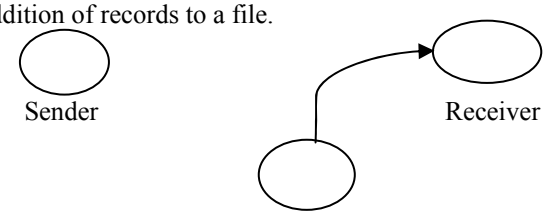
3.***Modification***: An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity.

e.g., changing values in data file, altering a program, modifying the contents of messages being transmitted in a network.



4. ***Fabrication:*** An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity.

e.g., insertion of spurious message in a network or addition of records to a file.



VIII. CRYPTOGRAPHIC ATTACKS-

1.Passive Attacks: Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Passive attacks are of two types:

a. ***Release of message contents:*** A telephone conversation, an e-mail message and a transferred file may contain sensitive or confidential information. We would like to prevent the opponent from learning the contents of these transmissions.

b. ***Traffic analysis:*** If we had encryption protection in place, an opponent might still be able to observe the pattern of the message. The opponent could determine the location and identity of communication hosts and could observe the

frequency and length of messages being exchanged. This information might be useful in guessing the nature of communication that was taking place. Passive attacks are very difficult to detect because they do not involve any alteration of data. However, it is feasible to prevent the success of these attacks.

2. ***Active attacks:*** These attacks involve some modification of the data stream or the creation of a false stream. These attacks can be classified in to four categories:

a. ***Masquerade*** – One entity pretends to be a different entity.

b. ***Replay -*** involves passive capture of a data unit and its subsequent transmission to produce an unauthorized effect. Modification of messages – Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect.

c. ***Denial of service*** – Prevents or inhibits the normal use or management of communication facilities. Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance. It is quite difficult to prevent active attacks absolutely, because to do so would require physical protection of all communication facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them.

IX.SYMMETRIC AND PUBLICKEY ALGORITHMS:

Encryption/Decryption methods fall into two categories.

1. Symmetric key
2. Public key

In symmetric key algorithms, the encryption and decryption keys are known both to sender and receiver. The encryption key is shared and the decryption key is easily calculated from it. In many cases, the encryption and decryption keys are the same.

In public key cryptography, encryption key is made public, but it is computationally infeasible to find the decryption key without the information known to the receiver.

A message is to be transferred from one party to another across some sort of internet. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.

Using this model requires us to:

– design a suitable algorithm for the security transformation

– generate the secret information (keys) used by the algorithm

– develop methods to distribute and share the secret information

– specify a protocol enabling the principals to use the transformation and secret information for a security service. Using this model requires us to:

– select appropriate gatekeeper functions to identify users

– implement security controls to ensure only authorized users access designated information or resources.

X. CONVENTIONAL ENCRYPTION

This type of encryption referred conventional (or) private-key (or) single-key and Sender and recipient share a common key. All classical encryption algorithms are private-key was only type prior to invention of public key in 1970 "plaintext - the original message"

Here the original message, referred to as plaintext, is converted into apparently random nonsense, referred to as cipher text. The encryption process consists of an algorithm and a key. The key is a value independent of the plaintext. Changing the key changes the output of the algorithm. Once the cipher text is produced, it may be transmitted. Upon reception, the cipher text can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption. The security depends on several factors. First, the encryption algorithm must be powerful enough that it is impractical to decrypt a message on the basis of cipher text alone. Beyond that, the security depends on the secrecy of the key, not the secrecy of the algorithm.

Two requirements for secure use of symmetric encryption: –

A strong encryption algorithm – A secret key known only to sender / receiver

$Y = EK(X)$ $X = DK(Y)$

Assume encryption algorithm is known then implies a secure channel to distribute key A source produces a message in plaintext, X = [X1, X2… XM] where M are the number of letters in the message. A key of the form K = [K1, K2… KJ] is generated. If the key is generated at the source, then it must be provided to the destination by means of some secure channel.

With the message X and the encryption key K as input, the encryption algorithm forms the cipher text Y = [Y1, Y2, YN]. This can be expressed as $Y = EK(X)$. The intended receiver, in possession of the k e y , is able to invert the transformation: $X = DK(Y)$

An opponent, observing Y but not having access to K or X, may attempt to recover X or K or both. It is assumed that the opponent knows the encryption and decryption algorithms. If the opponent is interested in only this particular message, then the focus of effort is to recover X by generating a plaintext estimate. Often if the opponent is interested in being able to read future messages as well, in which case an attempt is made to recover K by generating an estimate.

XI. CLASSICAL ENCRYPTION TECHNIQUES -

There are two basic building blocks of all encryption techniques: ***substitution and transposition.***

Substitution Techniques: A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing

plaintext bit patterns with cipher text bit patterns.

Caesar cipher (or) shift cipher: The earliest known use of a substitution cipher and the simplest was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing 3 places further down the alphabet.

e.g., plain text : pay more money

Cipher text: SDB PRUH PRQHB

Note that the alphabet is wrapped around, so that letter following „z" is „a".

For each plaintext letter p, substitute the cipher text letter c such that C = E(p) = (p+3) mod 26

A shift may be any amount, so that general Caesar algorithm is C = E (p) = (p+k) mod 26 Where k takes on a value in the range 1 to 25.

The decryption algorithm is simply P = D(C) = (C-k) mod 26

Playfair cipher: The best known multiple letter encryption cipher is the playfair, which treats digrams in the plaintext as single units and translates these units into cipher text digrams. The playfair algorithm is based on the use of 5x5 matrix of letters constructed using a keyword. Let the keyword be „monarchy". The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetical order. The letter „i" and „j" count as one letter. Plaintext is encrypted two letters at a time.

According to the following rules:

1. Repeating plaintext letters that would fall in the same pair are separated with a Filler letter such as „x".

2. Plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row following the last.

3. Plaintext letters that fall in the same column are replaced by the letter beneath, with the top element of the column following the last. Otherwise, each plaintext letter is replaced by the letter that lies in its own row And the column occupied by the other plaintext letter.

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Plaintext = meet me at the school house

Splitting two letters as a unit => me et me at th es ch o x ol ho us ex

Corresponding cipher text => CL KL CL RS PD IL HY AV MP HF XL IU

2. Strength of playfair cipher:

Playfair cipher is a great advance over simple mono alphabetic ciphers. Since there are 26 letters, 26x26 = 676 diagrams are possible, so identification of individual diagram is more difficult.

Polyalphabetic ciphers: Another way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message. The general name for this approach is polyalphabetic cipher. All the techniques have the following features in common. A set of related monoalphabetic substitution rules are used A key determines which particular rule is chosen for a given transformation.

Vigenere cipher: In this scheme, the set of related monoalphabetic substitution rules consisting of 26 caesar ciphers with shifts of 0 through 25. Each cipher is denoted by a key letter. e.g., Caesar cipher with a shift of 3 is denoted by the key value 'd" (since a=0, b=1, c=2 and so on). To aid in understanding the scheme, a matrix known as vigenere tableau is Constructed each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to its left. A normal alphabet for the plaintext runs across the top.

The process of Encryption is simple: Given a key letter X and a plaintext letter y, the cipher text is at the intersection of the row labeled x and the column labeled y; in this case, the ciphertext is V. To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword.

e.g., key = d e c e p t i v e d e c e p t i v e d e c e p t i v e

PT = w e a r e d i s c o v e r e d s a v e y o u r s e l f

CT=ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Decryption is equally simple. The key letter again identifies the row. The position of the cipher text letter in that row determines the column, and the plaintext letter is at the top of that column.

Strength of Vigenere cipher is One there are multiple cipher text letters for each plaintext letter and Letter frequency information is obscured.

One Time Pad Cipher: It is an unbreakable cryptosystem. It represents the message as a sequence of 0s and 1s. this can be accomplished by writing all numbers in binary, for example, or by using ASCII. The key is a random sequence of 0"s and 1"s of same length as the message.

Once a key is used, it is discarded and never used again. The system can be expressed as Follows:

Ci = Pi Ki Ci - ith binary digit of cipher text Pi - i th binary digit of plaintext Ki - ith binary digit of key Exclusive OR operation

Thus the cipher text is generated by performing the bitwise XOR of the plaintext and the key. Decryption uses the same key. Because of the properties of XOR, decryption simply involves the same bitwise operation: Pi = Ci Ki

e.g., plaintext = 0 0 1 0 1 0 0 1

Key = 1 0 1 0 1 1 0 0

---------- ciphertext = 1 0 0 0 0 1 0 1

Advantage: Encryption method is completely unbreakable for a ciphertext only attack.

Disadvantages It requires a very long key which is expensive to produce and expensive to transmit. Once a key is used, it is dangerous to reuse it for a second message; any knowledge on the first message would give knowledge of the second.

XII. TRANSPOSITION TECHNIQUES

All the techniques examined so far involve the substitution of a cipher text symbol for a plaintext symbol. A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

Rail fence is simplest of such cipher, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

Plaintext = meet at the school house

To encipher this message with a rail fence of depth 2, we write the message as follows:

m e a t e c o l o s e t t h s h o h u e

The encrypted message is MEATECOLOSETTHSHOHUE

Row Transposition Ciphers: A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of columns then becomes the key of the algorithm.

e.g., plaintext = meet at the school house

Key = 4 3 1 2 5 6 7

PT = m e e t a t t h e s c h o o l h o u s e

CT = ESOTCUEEHMHLAHSTOETO

A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext. The transposition cipher can be made significantly more secure by performing more than one stage of transposition. The result is more complex permutation that is not easily reconstructed.

XIII. NETWORK SECURITY ISSUES, THREATS AND SOLUTIONS

Now a day an industry, too many people continue to make the same mistakes with their network security over and over again, and it seems like we just aren't learning our lesson. It was Einstein who once said, "You cannot solve problems by using the same kind of thinking that we used when we created them," meaning, if a dilemma arises, you can't hope to fix it and keep it fixed without changing our methods. We all seem to fall into one or more of these habits over time, so to help remind us all of what we need to look out for, therefore we have some common **network security issues and solutions**.

1. **Non-complex or Weak Network Access Passwords**

Most network system administrators are open to an "old school" exploit known as ***brute forcing***. In order to correct this network security password vulnerability, they have implemented "CAPTCHA Technology." A common type of CAPTCHA requires the user to type letters or digits from a distorted image that appears on screen, which is commonly used to prevent unwanted internet bots from accessing websites and networks. This technology has given network security administrators a false sense of security, in regard to countering brute forcing.

The solution for the above issue is a ***complex password***. In order to create a complex password, you need seven or more characters combined with at least three numbers and one special character (capital letters, @ or # signs, etc.). Network security administrators should require the creation of complex passwords as well as implement a password expiration system to help remind users to change their passwords often. A restriction on how soon a password can be reused is also another handy precaution, that way someone isn't cycling between two different passwords every month or so.

2. Outdated Server Application or Software

Companies constantly release patches in order to ensure that our system is not vulnerable to new public threats. Hackers consistently release new threats and exploits which could allow harm to befall our network if these patches are not in place.

A simple solution is to ensure our system administrator is regularly informed of new threats and is updating our applications on a monthly basis.

3. Web Cookies

Although cookies do not carry viruses and cannot install malware on the host computer, the tracking of cookies and third-party tracking cookies are commonly used ways to compile records of individuals' browsing histories. Unencrypted cookies are a major network security issue because they can open our system to a XSS (Cross Site Scripting) vulnerability and that is a major privacy concern. With 'Open Cookies' anyone could have access to any login data cookies (saved password sessions) on the network, which creates a major vulnerability on our network security system.

The solution is to ensure all of our network cookies are encrypted and have an encoded expiration time. our network administrator should also force users to re-login any time they are accessing sensitive directories in our network.

4. Plain Hashes

"Anyone who knows their stuff can decrypt a Hash that is not Salted".

Hashing is used to index and retrieve items in a database and Plain Hashes are also used in many encryption algorithms. A Salt (which is another type of encryption) is added to Hashes in order to make a lookup table assisted Directory Attack (or Brute-Force) impractical or extremely difficult, provided the Salt is large enough. Basically, an attacker wouldn't be able to use a pre-computed look up table to assist in exploiting our network, which adds a whole new level of complexity to our network security system. So even if an attacker gains access and compromises our database (table), it will still be very difficult for the attacker to retrieve the information.

The best way to ensure safety in regard to Hashes is for our network administrator to hide the Salt (or encryption key), because if the hacker is able to gain access to our Salt encryption they can access our network system. Salt all of our Hashes. No Salt means no security.

5. Share Hosting (not Cloud Server Base)

suppose we are running a legitimate business and have a website with access to our internal network, Shared Hosting is not the way to go! A shared web hosting service is where many websites reside on one web server connected to the Internet. Each site sits on its own partition, or section or space on the server, to keep it separate from other sites. This

is generally the most economical option for hosting, because people share the overall cost of server maintenance. Think of it this way: shared hosting is like sharing a house with other people, and if someone breaks into our roommate's bedroom or any other area of the home for that matter, they'll also be able to access our own room!

This same concept is applied to Shared Hosting. When an attacker is inside one area of the shared server, it's almost as if they have a skeleton key that fits all of the locks. The best solution is to have dedicated Server Hosting and/or Secure Cloud Hosting.

XIV. **NETWORK SECURITY THREATS AND SOLUTIONS**

with increasing amount of people getting connected to networks, the security threats that cause massive harm are increasing also. Network security is a major part of a network that needs to be maintained because information is being passed between computers ets. and is very vulnerable to attack. Over the past five years people that manage network security have seen massive increase of hackers and criminals creating malicious threats that have been pumped into networks across the world.

According to ITSecurity.com the following are ten of the major network threats:

1. ***Viruses and Worms:*** A virus is a "program or piece of code that is loaded onto our computer without our knowledge and runs against our wishes". this can cause a huge amount of damage to computers. An example of a virus wouldbe if we opened an email and a malicious piece of code was downloaded onto our computer causing our computer to freeze.

in relation to a network, if a virus is downloaded then all the computers in the network would be affected because the virus would make copies of itself and spread itself across networks.

A worm is similar to a virus but a worm can run itself whereas a virus needs a host program to run

Soution: Install a security suite, such as Kaspersky Total Protection, that protects the computer against threats such as viruses and worms.

2. ***Trojen Horses:*** A Trojen Horse is "a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as running the file allocation of our table.

In a network if a Trojen horse is installed on a computer and tampers with the file allocation table it would cause a massive amount of damage to all computers of that network.

Solution: Security suites, such as Norton Internet Security, will prevent you from downloading Trojen Horses.

3. ***SPAM:*** SPAM is "flooding the internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it.

we believe that SPAM would not be the biggest risk to a network because even though it may get annoying and plentiful is still does not destroy any physical elements of the network.

Solution: SPAM filters are an effective way to stop SPAM, these filters come with most of the e-mail providers online. Also we can buy a variety of SPAM filters that work effectively.

4. ***Phishing:*** phishing is " an e-mail fraud method in which the perpetrator sends out legitimate - looking emails in an attempt to gather personal and financial information from recipients.

It is one of the worst security threats over a network because a lot of people that use computers linked up to a network are amateurs and would be very vulnerable to giving out information that could cause situations such as theft of money or identity theft.

Solution: Similar to SPAM use Phishing filters to filter out this unwanted mail and to prevent threat.

4. ***Packet Sniffers:*** "A packet sniffer is a device or program that allows eavesdropping on traffic travelling between networked computers, The packet sniffer will capture data that is addressed to other machines, saving it for later analysis.

In a network a packet sniffer can filter out personal information and this is a major security threat to a network.

Solution: "When strong encryption is used, all packets are unreadable to any but the destination address, making packet sniffers useless.

6. Maliciously Coded Websites: Some websites across the net contain code that is malicious. Malicious code is "Programming code that is capable of causing harm to availability, integrity of code or data, or confidentiality in a computer system". According to a survey AVG report that "300,000 infected sites appear per day.

Solution: Using a security suite, such as AVG, can detect infected sites and try to prevent the user from entering the site.

7. Password Attacks: Password attacks are attacks by hackers that are able to determine passwords or find passwords to different protected electronic areas.

Many systems on a network are password protected and hence it would be easy and steal data. This may be the easiest way to obtain private information because we are able to get software online that obtains the password for us.

Solution: At present there is no software that prevents password attacks.

8. Hardware Loss and Residual Data Fragments: Hardware loss and residual data fragments are a growing worry for companies, governments etc. an example this is if a numberof laptops get stolen from abank that have client details on them, this would enable the thief's to get personal information from clients and may be steal the clients identities.

Solution: This is a growing concern and as of present the only solution is to keep data and hardware under strict surveillance.

9. ***Shared Computers:*** shared computers involve sharing a computer with one or more people.

The following are a series of tips to follow when sharing computers are used

a. Do not check the "Remember my ID on this computer" box

b. Never leave a computer unattended while signed in

c..Always sign out completely

d. Clear the browser cache.

e. Keep an eye out for "shoulder suffers".
f. Avoid Confidential transactions.
g. Be wary of Spyware
h. Never save passwords.
i. Change your password often.

10.***Zombie Computers And Botnets:*** "A Zombie computer, or "drone" is a computer that has been secretly compromised by hacking tools which allow a third party to control the computer and its resources remotely". A hacker could hack into a computer and control he computer and obtain data.

Solutions: Antivirus software can help prevent zombie computers.

A botnet is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions to other computers on the internet".

This is a majorsecurity threat on a network because the network, unknown to anyone, could be acting as a hub that forwards malicious files ets to other computers.

Solution: Network Intrusion Prevention (NIP) system can help prevent botnets.

APPENDIX:

01. Cryptography- The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and the retransforming that message back to its original form.
02. Plain Text- The original intelligible message.
03. Cipher text- the transformed message
04. Cipher - An algorithm for transforming an intelligible message into one that is unintelligible by transposition and / or substitution methods.
05. Key - Some critical information used by the cipher, known only to the sender & reciver
06. Enciper (Encode)- The process of converting plain text to cipher text using a cipher and a key.
07. Decipher (Decode) - The process of converting cipher text back into plaintext using a cipher and a key.
08. Cryptanalysis- the study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key. Also called Code Breaking.
09. Cryptology - Both Cryptography and Cryptanalysis.
10. Code - An algorithm for transforming an intelligible message into an unintelligible one using a code-book.
11. ***cipher text*** - the coded message
12. ***Cipher*** - algorithm for transforming plaintext to cipher text ***Key*** - info used in cipher known only to sender/receiver
13. ***encipher (encrypt)*** - converting plaintext to cipher text
14. ***decipher (decrypt)*** - recovering cipher text from plaintext 15. ***Cryptography*** - study of encryption principles or methods 16. ***Cryptanalysis (code breaking)*** - the study of principles or methods of deciphering cipher text without knowing key 17. 17. ***Cryptology*** - the field of both cryptography and cryptanalysis.

REFERENCES

1. Cryptography and Network Security – by Atul Kahate – TMH.
2. Data Communications and Networking- by Behourz A Forouzan
3. Cyber Security Operations Handbook – by J.W. Rittiaghouse and William M.Hancok – Elseviers.
4. ITSecurity. (2007) Network Security Threats for SMBs. Available at http://www.itsecurity.com /features /network- security-threats-011707
5. Webopedia. (2007) *virus* Available at http://www. webopedia.com /TERM/v/virus.html
6. Trend Micro. (2008) Network viruses. Available at: http://us.trendmicro.com /us /threats /enterprise /glossary /n network-viruses/index.php
7. Symantec. (2007) Trojen Horse. Available at: http:// www.symantec.com /security_response/ writeup.jsp?
8. Search Security. (2003) phishing. Available at: http: //searchsecurity.techtarget.com/ sDefinition/0,,sid 14_gci916037,00.html.
9. Wise Geek (2009) what is a Packet Sniffer? Available at: http://wisegeek.com/what-is-a-packet -sniffer.html
10. Wise Geek (2009) what is a Zombie Computer? Available at: http:// wisegeek.com what-is-a-zombie-computer. html