Odyssey Of Data Security With A New Perception

Ankita[1], Lavisha[2]
[1] Computer Science Department, GGS Inderprastha University, Institute of Innovation in Technology and Management
Janak Puri, New Delhi-110058, India

[2] Computer Science Department, GGS Inderprastha University, Institute of Innovation in Technology and Management
Janak Puri, New Delhi-110058, India

Abstract

Maintaining the security of the data is one of the most important and critical task organizations are facing today. This is due to the fact that the data are accessed by both types of users; first, those users who are authorized to do so and who needs to access the data for making sure that everything works well. And second, those who are not authorized to access the data, they may be in-house employees of the organizations, some outsiders, malicious users who may want to access the sensitive information and take advantage of it. So, the problems of data security need to be addressed especially in this mobile environment.

This chapter proposes solutions to data security problem by various ways so that even if any unauthorized user is able to access the data, he will only get the data in an un-understandable form and not the actual data.

1. Introduction

Why do we keep our jewellery and other valuable things in a locker? Why do we need to lock the front door of our home? Why do we lock our car while parking? The answers to all these questions are - for security reasons. We take basic precautions to protect our valuables. Similarly, information is also a valuable asset.

1.1 Invention of Information

Latin language introduced the word Information. The verb from which it has been taken out is “informare”, which means ‘to instruct’. In other words it means giving a new angle to an existing idea or fact.

1.2 Are data and information same?

Table 1: Data v/s Information

Data	Information
Data is raw, unorganized facts or figures that needs to be processed.	After processing of data, journey of information begins.
Data is simply an input given.	Information is an output according to the given data.
Data is random and do not follow any pattern.	Information is processed data and hence it is in arranged form and do follows a pattern.
Data is not in structured form.	Information is structured form of data.

1.3 Sources of data and information

Data can be gathered from internal and external sources. External sources are like market research, government policies, market share etc. whereas internal sources are within the business.

1.4 Why is information security important – need for information security

Threats to information system may come from internal or external sources in the form of intentional or accidental threats.

1.5 What is information security?

Information security is not another name for computer security. Computer security is concerned with security from unauthorized users approach and practice, whereas information security is concerned with information maintenance, information confidentiality and data purity.

1.6 Practicing better information protection

No system is totally secure. The exposure of unauthorized persons has greatly increased as networks are no more confined to individual departments or groups. It is very difficult to assert control over networks especially when thousands of people can access a network from many remote locations. Information security refers to precautions taken to keep information safe from unauthorized access.

2. Ways to protect data

Some ways to protect confidential and valuable data from loss or unauthorized access are:

1. On regular intervals take back up
2. Use file level security
3. Use password mechanism
4. Use EFS Encryption
5. Use disk encryption
6. Use PKI
7. Use steganography
8. Use IPsec protocol
9. Use wireless transmission
10. Use RMS

2.1 On regular intervals take back up

The most important step in protecting data from loss is to back it up regularly.

Frequency at which data needs to be backed up depends on the requirements of the user. Sometimes work done in a week's time is the most important one which needs to be saved. On the other hand, a day's work or an hour's work needs to be backed up.

Nowadays there are many options available for backing up our data like CD, DVD, external hard drives, flash drives.

Windows also provide backup utility to perform backups. It provides a user with 2 options:

1. wizard mode
2. manually

2.1.1 Wizard mode

Wizard mode is the simplest one because in this, the user just has to follow the pre defined steps to complete the back up.

2.1.2 Manual Mode

For doing back up manually, user needs to configure the backup settings and then can do scheduling for getting the backup on regular intervals.

2.2 Use file-level security

In network shares, setting the share permissions, control user access to the files available on the net.

File-level permissions are used when we are sharing the system with users also. File level permissions are also known as NTFS permissions.

There are two ways for setting security permissions on the files and folders:

a. On the sharing flap of the file's or folder's property panel by clicking the permissions button.
b. On the security tab of the file's or folder's properties sheet.

2.3 Use password mechanism

Microsoft Office applications allow us to set user defined passwords at document level. To open the document, we need to enter the preset password. To protect a document using this method, in Microsoft Word 2007, go to round office button | prepare and click the encrypt document, it will ask for a password which will be saved for future references.

Setting a password protection is easy but cracking a password is easier. There are softwares in the market which can recover passwords, such as Rixler software and many more. Various zipping softwares can also be used like WinZip, 7-Zip etc.

2.4 Use EFS encryption

Encrypting File System (EFS) is a feature to store files and folders in an encrypted format on our hard disk. Encryption is defined as a way of converting data into a format that cannot be read by others. Encrypting file system automatically encrypts our data when it is stored on the hard disk. The Encrypting file system method is not available in Windows Extra Professional version.

File system is defined as a system that an Operating System or program uses to organize and keep track of files.

Operating systems do have its own file management system; still a separate file management system can be bought.

Some of the File systems in any OS are:

a. FAT (File Allocation Table)
b. HPFS (High Performance File System)
c. NTFS (New Technology File System)

Microsoft-Disk operating system and earlier versions of windows, windows new technology and windows XP permits exercise of FAT-16 or FAT-32.

DOS and Linux support HPFS whereas Windows New Technology and Windows Extra Professional version uses NTFS.

2.4.1 Steps to Encrypt a File or a folder

Minimum requirement for encrypting a file or folder is the presence of the NTFS file system.

In order to encrypt a file:

1. Click Start | All Programs, go to Accessories, and click Windows Explorer.
2. Search for the file that you want, right-click on it, and then click Properties.
3. On the General tab, click Advanced.
4. Under Compress or Encrypt attributes, choose the "Encrypt contents to secure data" option.
5. Click OK.

Once encryption is done, an unauthorized user can't open the file. In trying to do so, the following message will appear:

"User name does not have access privileges and word cannot open the document."

The following message will appear whenever a user move that document to any other location:

"You do not have sufficient access for this."

2.4.2 Steps to Decrypt a File or a folder

For decrypting a folder, same steps are used but in reverse order:

1. Click on properties button by performing the right click button on that folder.
2. Now click on advanced button.
3. For decryption, uncheck the Encrypt contents to secure data check box.
4. Now close the advanced dialog box and properties dialog box.
5. The Confirm Attribute Changes dialog box appears when the folder has files in it.
6. In order to decrypt all contents of a folder select "Apply Changes to this folder, subfolders and files".
7. Select ok.

2.5 Use disk encryption

Disk encryption, itself means encryption of an entire physical or logical disk.

Disk encryption can be defined as a technology which protects information from unauthorized user by converting it into unreadable code that cannot be deciphered easily. Disk encryption makes use of either disk encryption software or hardware to encrypt every bit of data that goes on a disk or disk volume.

In full disk encryption, all information stored on the disk is encrypted except master boot record. If a user wants to include MBR as a part of encryption then, hardware-based full disk encryption technology can be used.

2.5.1 How Full Disk Encryption Works

Full disk encryption uses encryption algorithms that assist in encrypting data when it gets stored on the hard drive or other movable storage device. This type of encryption system makes sure that encryption of data does not slip from user's mind or select only pieces of data to be encrypted.

2.5.2 Shortcomings of Full Disk Encryption

One shortcoming of full disk encryption is that no encryption of data is done when transmission is taking place i.e. when the information is being sliced between devices or stored on movable devices like a flash drive or external hard drive. Secondly, it does not take care of the data that is being transmitted over the email from a computer that comprises of full disk encryption.

Sometimes to boot up the system the entire system needs to be decrypted which requires decryption key.

2.5.3 Advantages of Full Disk Encryption

Full Disk Encryption decreases the pressure on the user to identify which files need to be encrypted for data protection. This means all the files present on the hard drive are automatically encrypted and for accessing such type of files, a password or smart card is required. Encrypted files include the file containing sensitive data, which are temporary files.

Full Disk Encryption also avoids the unauthorized user from grabbing the data with a microprocessor card. The microprocessor card is the authentication device that grants the system to reacquire the key that will decode the files on the hard drive. The key acts as a safeguard because the data can instantaneously be relinquished by eradicating the cryptography key.

These types of systems provide all of the functions to be controlled from a leading location within the organization. Various functions provided by these systems include managing the key used for decryption, limiting the command to the movable devices, mentioning and recreation of missed passwords or microprocessor cards.

Examples include PGP Whole Disk Encryption and DriveCrypt etc.

2.6 Use PKI

PKI stands for Public Key Infrastructure. This technology requires a pair of keys, out of which one key is used for encrypting the information and the other key is used for decryption. One of the 2 keys is made public whereas the other is kept secret, which is known as private or secret key. In view of the fact that anyone may attain the public key, users may commence safe conversation without having to share a secret beforehand through some other medium with their contributor. The Infrastructure is the elementary system which is required for issuing keys and certificates and to publish the public information.

2.6.1 Public Key Certificates

A public key has an attribute attached with it i.e. name of its owner. Attributes are attached with a key using certificate, called public key certificate (PKC). PKC is a digitally signed document that assists in validating the sender's authorization and name. Nowadays, other names used for Public Key Certificates are digital certificate or identity certificate.

Some of the Contents of a public key certificate are:

1. Unique id of the certificate
2. Name of the owner,
3. Public key and e-mail id of the owner,
4. Dates regarding the certificate, mentioning valid from and valid to dates
5. Aim of the public key, etc.

This public key certificate is signed by the issuer with his private key. By this, identity of the issuer can be verified by the intended receiver. This technique ensures the receiver that the contents have not been changed or altered.

2.6.2 Role of public and private key on sender/receiver's side

Table 2: Role of Keys

Function to be performed by the key	Key used	Receiver or sender side??
Data encryption on the receiver's side	Public key	Receiver
Sign data	Private key	Sender
Data decryption on the receiver's side	Private key	Receiver
Verify a signature	Public key	Sender

2.6.3 Limitations of PKI

Some of the disadvantages of PKI systems are:

1. They are obscure and uneconomical
2. Require extensive planning
3. Not easily maintainable
4. Installation and deployment is also very hard.

2.7 Use steganography

Steganography consists of 2 words viz. STEGANOS which means "Covered" and GRAPHIE means "Writing".

Steganography is a technique through which a sender can send the concealed message in such a way that only the dedicated receiver is aware about the prevailing of the concealed message.

For example, a text message can be masked behind a text, picture, audio-visual file etc.

2.7.1 Working of steganography technique

Steganography is often used in conjunction with any encryption software. In this, data is encrypted first and then concealed inside another file with the help of steganography software.

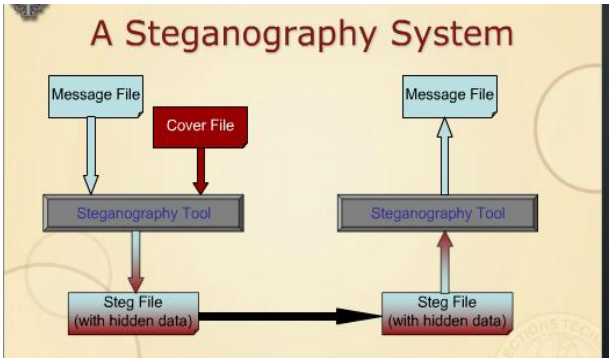

Fig 1: Steganography technique

Steganography and cryptography are two sides of a coin.

The goal of cryptography is to make data unreadable by unauthorized group, i.e. to make the data invisible for unauthorized group.

One of the famous examples of steganography software is Quickstego software by quickcrypto that will encrypt messages and lets you keep the text shielded in pictures.

2.8 Use IPSec protocol

IPSec is commercially established set of rules. Its assistance is based on cryptography. The main reason for using data encryption is to protect the data while it is travelling in an IP network.

It is designed in such a way that it provides unique identification of the sender, authenticity of the data and maintains privacy of data.

It operates at the 3rd layer of OSI model i.e. at network layer. IPSec when compared with Secure Socket Layer comes out to be much more advantageous.

2.8.1 Architecture of Internet Protocol Network

IPsec Architecture included many theorems and formulas.

The relationship can be depicted by following figure:

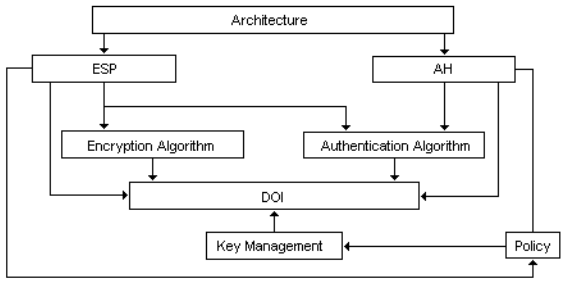

Fig 2: IPsec Protocols

The above figure shows that IP Sec is not a single protocol. It consists of 2 protocols, which can be used independently or in collaboration:

The first one is AH and second is ESP.

2.8.1.1 AH (Authentication Header)

1. It is used to validate the identification of the sender.
2. It provides purity of the data to ensure that it hasn't been altered.
3. It is not concerned with encryption of data.
4. It provides no privacy.
5. AH signs the entire packet.

2.8.1.2 ESP (Encapsulating Security Payload)

1. It provides privacy by encrypting the data itself, along with validation and purity.
2. It signs only the data, without signing the packet.

2.8.2 Modes of operation for AH & ESP

There are two modes of operation

1. Tunnel mode: It is used to create a VPN (virtual private network). It implements gateway-gateway& server-server protection.

2. Transport mode: It is used for encrypting the data residing in a tunnel. It implements end-to-end protection.

2.9 Use wireless transmission

Wireless security is basically a management issue. To connect your computers together through a wireless network is one of the easiest and least messy ways for wireless networking. Wireless networking provides many advantages, but it also has many new security threats. That does not mean we should not use wireless technology. We just have to be smart about it and take some basic precautions to make it more difficult for curiosity attackers to get into our personal information.

The simple steps or actions that we can take to secure our wireless network are:

1. Change the default SSID (Service Set Identifier) or ESSID (Extended Service Set Identifier).
2. Disable identifier broadcasting.
3. Enable encryption using WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access).
4. Restrict unnecessary traffic using Firewalls.
5. Change the default administrator password.
6. Protect your system by the help of updated anti-virus software.

Now, look at the some of the salient security threats of wireless systems are:

1. Accidental association
2. Malicious association
3. Ad-hoc networks
4. Non-traditional networks
5. Identity theft (MAC spoofing)
6. Man-in-the-middle attacks
7. Denial of service
8. Network injection
9. Caffe Latte attack

In summary, the nature of wireless communications creates three basic threats: Interference, Variation and Severance.

Following steps are taken for improving the management of wireless networks:

1. Have a complete knowledge of the topologies.

2. Maintain the records of all the devices which are used in networking.
3. Take backups of data.
4. Do security testing and assessment.
5. Do security audits.
6. Enhance security features for upgrading its version.

2.10 Use RMS

Microsoft Windows Rights Management Services (RMS) is a premium service that offers Information Protection Technology to help businesses prevent information leakage by applying persistent access rights to their digital assets.

Rights management can be used in many ways:

1. On setting only read rights to a word document which is being sent then that document can't be copied, changed or saved by the recipient.
2. We can set expiry date/time on documents so that the receiver can't access them after the set time.

RMS shields information in online mode as well as offline mode.

2.10.1Windows RMS Benefits

1. Protect Viewing and Usage
2. Flexible Technology
3. Persistent Usage Policies
4. Reliable Solutions

2.10.2Pre requisites of RMS

1. Server-Side

    1.1 Window Server 2003 Standard, Enterprise, Web or Datacenter Editions
    1.2 Windows RMS
    1.3 Active Directory service (Windows Server 2000 or later) to provide unique identification to every user.
    1.4 Database Server such as Microsoft SQL Server™ or MSDE to store configuration data and use license requests.

2. Client-Side

    2.1 Windows Rights Management client software.
    2.2 A RMS-enabled application or browser.

Many Microsoft products support RMS.

3. Futuristic approach of data security

Futuristic approach of data security takes minimum space and provides huge security is 3D Password.

Secure authentication scheme is one of the most important requirements of present time, now a day's online shopping , e marketing's and cloud computing etc becomes very familiar among the public. No doubt there are many validation methods already available and being used all over the world. In fact these preexisting validation methods have several liabilities.

3.1Drawbacks for Preexisting Security Mechanisms:

1. Textual passwords are easily guessable.
2. Applying biometrics on a user's personal characteristics is just unreliable, as human physical characteristics can change over time, if you are ill, your eyes may puffy or your voice may affected by throat infection or your fingers or your hands may rough due to any environmental condition then in all these types of cases it may be more difficult for the machinery to identify you accurately.
3. Smart Cards and Tokens can be easily stolen and duplicated.
4. The server needs to store the graphical pictures or portfolio images of each user in plain text; the process of selecting a set of pictures from the picture database can be tedious and time consuming for the user.

3.2 3D Password Technique

The 3D Password technique is a combination of the benefits of biometrics, possession & knowledge based authentication schemes.

Or we can say that the 3-D password is a combination of various validation schemes. For validation, a 3-D virtual environment is created in which the user deals

and communicates with various constructive objects. The sequence of actions and interactions made by the user while communicating with these objects sums up to create a 3d password.

Various validation techniques which are used nowadays are passwords containing alphabets, numbers or strings and various types of biometric devices which can be used while creating a 3-D artificial environment. The design of the 3-D environment and the type of objects selected determine the 3-D password key space.

For example, Let us assume that the user enters in the 3D office and turns around to the door located in (10, 24, 91) and opens it, then presses the door bell.

The user then finds a laptop towards the right hand side, which is placed in the position (4, 34, 18) and the user types "IITM". The user actions in the 3d virtual environment can be recorded as follows:

(10, 24, 91) action – opens the car door

(10, 24, 91) action – closes the car door

(4, 20, 25) action – Press door bell

(4, 34, 35) action – Typing "I"

(4, 34, 35) action – Typing "I"

(4, 34, 32) action – Typing "T"

(4, 34, 38) action – Typing "M"

All the activities done by the user in the performed sequence make his /her 3D password.

Hence, the following requirements are satisfied by this:

1. Its very difficult for intruders to guess the 3D password.
2. 3D Password is difficult to share with others.

3.3 Applications

1. In Server room
2. In Nuclear and military facilities
3. In Airplanes and jetfighters

3.4Advantages

1. The user can make his validation.
2. The validation can be advanced since the invalidate persons will not communicate with the same object as the validate person.
3. The virtual objects can be altered or changed.
4. The password would be very hard to break by using common algorithms.

3.5 Disadvantages

1. Requirement of huge memory.
2. Very costly.
3. Hardware dependent
4. Not user friendly, as a user needs to know how to use all kinds of devices like web camera or thumb reader.

4. Conclusion

Good security starts and ends with secrecy, purity, accessibility of the data. Nothing is 100% secured but still every data needs to be protected. This paper analyzes the 10 steps for an approach to secure data against insider and outsider threats and also it introduces new concept for securing data. Information should be protected according to its sensitivity, criticality and value. Confidential information should be stored and maintained only where the access can be adequately controlled. A data security program is essential for diminishing various threats and avoiding a data rupturing. Regular practicing of the security plan will decrease exposure to threats and will improve the overall safety of data.

References

[1] Dr.Sushila Madan, Management Information and Control Systems, Delhi, Taxmann Allied Services, 2007

[2] David Salomon, Data Privacy and Security, USA, Springer, 2003.

[3] William Easttom, Computer Security Fundamentals, USA, Pearson, 2011

Authors Biography

[1]Ms. Ankita, obtained her MCA degree from" Tecnia Institute of Advanced Studies", Delhi affiliated to "Guru Gobind Singh Inderprastha University", Delhi. She is working as "Assistant Professor" in department of Computer Science in "Institute of Innovation in Technology and Management", Delhi. Her area of Interest is in the field of Computer Network, Mobile Computing and Data Mining. She has attended various national conferences, seminars and workshop.

[2]Ms. Lavisha, obtained her MCA degree from" GVM Institute of Technology and Management",Sonepat affiliated to "Maharishi Dayanand University", Rohtak. She is working as "Assistant Professor" in department of Computer Science in "Institute of Innovation in Technology and Management", Delhi. Her area of Interest is in the field of Data Base Management System, Operating System and Computer Architecture. She has attended various national conferences, seminars and workshop.