CYBER SECURITY

FOR ALL PG STUDENTS

SRI GVG VISALAKSHI COLLEGE FOR WOMEN

UDUMALPET

LEVEL I:

M.A Economics/ History/ Literature/M.Com

LEVEL II:

M.Sc Mathematics/Physics/Computer Science

Sri GVG Visalakshi College for Women (Autonomous), Udumalpet - 642128

Re-Accredited by A++ in NAAC

An ISO Certified Institution

In House Edition, First Impression 2015

Revised Edition 2017

Course framed by

- Mrs. S.Kalaisevi, Associate Professor, Department of Mathematics
- Mrs. R.Jayalakshmi, Head & Assistant Professor, Department of B.Com(E.Com)
- Ms. R.Kavithamani, Assistant Professor, Department of Physics
- Mrs. V.Vadivu, Assistant Professor, Department of IT
- Mrs. J.Aishwarya Lakshmi, Assistant Professor, Department of BCA

Revised & Redesigned by

- Mrs. S.Shobana, Head & Assistant Professor, Department of Computer Science
- Mrs. B.Sasikala, Assistant Professor, Department of Computer Science
- Ms. G.Krishnaveni, Assistant Professor, Department of Computer Science
- Mrs. D.Pavithra, Assistant Professor, Department of Computer Science
- Mrs.N.Sathyapriya, Assistant Professor, Department of Computer Science
- Ms.E.Kokilamani, Assistant Professor, Department of Computer Science
- Ms.P.Yasodha, Assistant Professor, Department of Computer Science
- Ms.S.Ponmalar, Assistant Professor, Department of Computer Science
- Mrs.S.Mahalakshmi, Assistant Professor, Department of Computer Science
- Mrs.J.Rajeswari, Assistant Professor, Department of Computer Science
- Ms.R.Subhasree, Assistant Professor, Department of Computer Science
- Mrs.S.Saranya, Assistant Professor, Department of Computer Science
- Mrs.G.Kowsalya, Assistant Professor, Department of Computer Science

Preface

Today, cyber security is widely viewed as a matter of pressing national importance. Many elements of cyberspace are notoriously vulnerable to an expanding range of attacks by a spectrum of hackers, criminals, terrorists, and state actors. For example, government agencies and private-sector companies both large and small suffer from cyber thefts of sensitive information, cyber vandalism (e.g., defacing of Web sites), and denial-of-service attacks.

The nation's critical infrastructure, including the electric power grid, air traffic control system, financial systems, and communication networks, depends extensively on information technology for its operation. National policy makers have become increasingly concerned that adversaries backed by considerable resources will attempt to exploit the cyber vulnerabilities in the critical infrastructure, thereby inflicting substantial harm on the nation. Numerous policy proposals have been advanced, and a number of bills have been introduced in Congress to tackle parts of the cyber security challenge.

This book is designed to serve as the textbook for a one-semester course devoted to cyber security. It is focused on helping students acquired the skills sought in the professional workforce.

M.A Economics/ History/Literature

Semester - II

Cyber Security 15MGCS

Level - I

(For the students admitted from the academic year 2015-2016 onwards)

[30 Hours]

Unit I

Introduction - Cyber law - Features of Cyber Law - Significance of Cyber Law - Advantages. Data Security - Meaning - Fundamentals of Data Security - Requirements of Data Security - Precautionary Measures.

Unit II

Cyber Security: Introduction in Cyber Security - Hackers - Attackers - Types of Attackers Examples - Data Recovery.

Unit III

Authentication - Authentication Control- User name and Password - Protecting Passwords -Examples.

Books for Reference

1. "Cyber law: The Law of Internet", Jonathan Rosenoer, Springer Verlog, 1997
2. "Cyber Security Operations Handbook", John W Ritting House, William M.Hancock, Read Elsevier 2008.
3. "Computer Security", Dieter Gollmann

M.Sc., Mathematics/Physics/Computer Science/M.Com

Semester - II

Cyber Security 15MGCS

Level - II

(For the students admitted from the academic year 2015-2016 onwards)

[30 Hours]

Unit I

Concept of Cyber law and Cyber Space: Introduction - Meaning and Features of Cyber law - Significance and Advantages of Cyber Law - Meaning of Cyber Space - Inclusive of Cyber Space - Facilitating Functions of Cyber Space - Major Issues in Cyber Space. Need for an Indian Cyber law: Plans of National Information Technology Policy (NITP) - Need for Protection of data - Transactions in Security - Electronic Banking.

Unit II

Hackers & its Types - Cracking - Pornography - Software privacy - Data Recovery - File Modification & File access, Recover Internet Usage Data, Recover Swap Files/Temporary/Cache Files, and Introduction to Encase Forensic.

Unit III

Firewalls - Authentication & Access Control: Identification - Authentication - Authentication by Passwords - Protecting Passwords - Access Control Structure - Evidences - Law of Evidence on Electronic Records.

Books for Reference

1. "Cyber law: The Law of Internet", Jonathan Rosenoer, Springer Verlog, 1997
2. "Cyber Security Operations Handbook", John W Ritting House, William M.Hancock, Read Elsevier 2008.
3. "Computer Security", Dieter Gollmann

M.A Economics/ History/ Literature/M.Com

Semester - II

Cyber Security 17MGCS

Level - I

(For the students admitted from the academic year 2017-2018 onwards)

Course Objective: [30 Hours]

- To provide students with a high level understanding of how information security functions in an organization.
- To master understanding external and internal threats to an organization.

Unit I:

Introduction - Cyber law - Features of Cyber Law - Significance of Cyber Law - Advantages. Data Security - Meaning - Fundamentals of Data Security - Requirements of Data Security - Precautionary Measures.

Unit II:

Cyber Security: Introduction in Cyber Security - Hackers - Attackers - Types of Attackers - Examples - Data Recovery.

Unit III:

Authentication - Authentication Control - User name and Password - Protecting Passwords -Examples.

Books for Reference:

1. Jonathan Rosenoer , "Cyber law: The Law of Internet", Springer Verlog, 1997.
2. John W Ritting House, William M.Hancock, "Cyber Security Operations Handbook", Read Elsevier 2008.
3. Dieter Gollmann , "Computer Security", Wiley Publication, Third Edition, 2013.

M.Sc Mathematics/Physics/Computer Science

Semester-II

Cyber Security 17MGCS

Level - II

(For the students admitted from the academic year 2017-2018 onwards)

Course Objective: [30 Hours]

- To provide deeper understanding into cyber law, its application, threats/vulnerabilities to networks and countermeasures.
- To gain knowledge about firewall, its working and Authentication mechanisms.

Unit I:

Concept of Cyber law and Cyber Space: Introduction - Meaning and Features of Cyber law - Significance and Advantages of Cyber Law - Meaning of Cyber Space - Inclusive of Cyber Space - Facilitating Functions of Cyber Space - Major Issues in Cyber Space. Need for an Indian Cyber law: Plans of National Information Technology Policy (NITP) - Need for Protection of data - Transactions in Security - Electronic Banking.

Unit II:

Hackers & its Types - Cracking - Pornography - Software privacy - Data Recovery - File Modification & File access, Recover Internet Usage Data, Recover Swap Files/Temporary/Cache Files, and Introduction to Encase Forensic.

Unit III:

Firewalls - Authentication & Access Control: Identification - Authentication - Authentication by Passwords - Protecting Passwords - Access Control Structure - Evidences - Law of Evidence on Electronic Records.

Books for Reference:

1. Jonathan Rosenoer, "Cyber law: The Law of Internet", Springer Verlog, 1997
2. John W Ritting House, William M.Hancock, "Cyber Security Operations Handbook", Read Elsevier 2008.
3. Dieter Gollmann, "Computer Security", Wiley Publication, Third Edition, 2013.

LEVEL I

In today's environment technology has made to access the information worldwide quicker and easier, telecommunication made everyone to capture, store and transmit the information to every nook and corner of the world. The rapid development of information technology provides new possibilities for automating tasks and enriching the lives of the people. Technology refers to methods, tools, procedures to handle applied input and output relations to perform a specific task.

Technology which is adopted to store, process and transmit the information from one place to another place is called information technology. Computer and other electronic devices like ATM mobile phones are used to store data, process data and transmit the data to the place we need.

Cyber means the use of Internet technologies and computers. It includes computers, networks, software, data storage devices, Internet, websites, emails, ATM machines etc. Cyber security is security applied to computers, computer networks, and the data stored and transmitted over them. The field is of growing importance due to the increasing reliance of computer systems in most societies.

Cyber space

Cyberspace is "the notional environment in which communication over computer networks occurs." It is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology (ICT), devices and networks.

Unlike most computer terms, "cyberspace" does not have a standard, objective definition. Instead, it is used to describe the virtual world of computers. For example, an object in cyberspace refers to a block of data floating around a computer system or network. With the advent of the Internet, cyberspace now extends to the global network of computers. So, after sending an e-mail to your friend, you could say you sent the message to her through cyberspace.

Cyber space is a domain characterized by the use of electronic and electromagnetic spectrum to store, modify and exchange data via network systems and associated physical infrastructure. The Cyber space is borderless and actions in the cyber space can be anonymous. These features are being exploited by adversaries for perpetration of crime in the cyber space. The scale and sophistication of the crimes committed in the cyber space is continually increasing thereby affecting the citizens, business and Government. As the quantity and value of electronic information have increased, the criminals and other adversaries embraced the cyber space as a more convenient and profitable way of carrying out their activities anonymously. Every action and reaction in cyberspace has some cyber legal perspectives. Cyber space includes Computer, Mobile phone, ATM, Data storage device, Software, Network, Website, E-mail

Cyber law

Cyber law is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less a distinct field of law in the way that property or contract are as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. Cyber law is an attempt to integrate the challenges presented by human activity on the Internet with legacy system of laws applicable to the physical world.

Cyber law is the law which regulates the operations performed by the user via network by electronic means. Cyber law is important because it touches almost all aspects of transactions and activities involving the internet, World Wide. In other words, we can say cyber law regulates the cyber space. Cyber means the use of Internet technologies and computers it includes

computers, networks, software, data storage devices, Internet, websites, emails, ATM machines etc. To protect the cyber crime over Internet, this law is passed to protect the Internet cyber crime. This law is approved by the government. Cyber law Includes: Cyber law encompasses laws relating to

- Cyber crimes
- Electronic and digital signatures
- Intellectual property
- Data protection and privacy

Features of cyber law:

Cyber law contains the following features:

- It contains a set of rules and guidelines.
- It defines the legal internet activities.
- It specifies the illegal activities which are punishable under law.
- It provides legal framework for all the activities which are carried out through the network.

Significance of cyber law:

Now, we are replaying upon information technology to carry out varies day to day operation. Information technology has varied applicability in almost all aspects of our life. Some of the areas are science and engineering, business, education and entertainment.

- Companies now are able to carry out electronic commerce using the legal infrastructure provided by the Act
- Act allows Government to issue notification on the web thus heralding e – governance.
- Protect Computer fraud and Unauthorized access.
- Consumers are now increasingly using credit cards for shopping.
- Most people are using email, cell phones and SMS messages for communication as well as Deal with Internet Banking Transactions.

Though we are utilizing information technology frequently in some of the areas, we have to be equally caution. For example, due to the anonymous nature of the internet, it is possible for the fraudulent people to involve in several of criminal activities. Some of the criminal activities are

1. Launching of malicious software in the form of worms, viruses, Trojans, spyware, adware, etc,
2. Computer hacker to break into computer system, especially to get secret information.
3. Downloading unauthorized software.
4. Selling illegal articles such as narcotics, weapons, etc.,
5. Gambling activities through online.
6. Stealing of money from banks using networks.
7. Credit card frauds.
8. Cyber stalking, cyber defamation, indecent & abusive mails.
9. Stealing the business secrets and documents.
10. Stealing of data in BPO centers.
11. Stating false advertisements in the web page, e-mail and SMS.

To overcome the above said criminal activities, varies security measures are applied. Still, lots of cyber crimes are going on. So, there is a need for cyber law.

Advantages of cyber law

Cyber law has the following advantages:

1. Cyber law regulates the transaction which is carried out through cyber space.
2. It provides legal infrastructure for e-Commerce transactions.
3. It authorized the certifying authorities for issuing digital signature certificates.
4. It validates the digital signature.
5. E-mail is considered as a valid message and legally acceptable in a court of law.
6. It is possible for the users to use against the fraudulent people who commit cyber crimes and cause losses.
7. Statutory remedy is available for any losses which occur due to cyber crimes.

Facilitating function of cyber law

Today adversaries are developing, selling and distributing malicious code with ease, maximizing their gains and exploiting the fact that attribution is a challenge. E-business, e-banking, e-shopping, e-receipts & payments, e-transmission of the documents, e-education, e-medicine, e-information, e-database, e-entertainment, e-engineering are the major functions of cyber law.

Application of cyber law

Electronic Banking

Cyber Law has a very vital role to play at the application level, because of the critical nature of financial data transfer. The financial messages should have the under noted features:

- The receipt of the message at the intended destination (data transmission)
- The content of the message should be the same as the transmitted one (data integrity)
- Sender of the information should be able to verify its receipt by the recipient (data acknowledgement)
- Recipient of the message could verify that the sender is indeed the person (data authenticity)
- Information in transit should not be observed, altered or extracted (data security)
- Any attempt to tamper with the data in transit will need to be revealed (data security)
- Non-repudiation (non repudiation of the data)

These features take down essentially to

- Authentication
- Authorization
- Confidentiality
- Integrity
- Non-repudiation

Authentication:

To verify the identity of the sender of the message to the intended recipient to prevent spoofing or impersonation.

Authorization:

Authorization means to control the access to specific resources for unauthorized persons

Confidentiality:

To maintain the secrecy of the content of transmission between the authorized parties. Confidentiality is the concealment of information or resources'. The need for keeping the information secret arises from the use of computers in sensitive fields such as government and industry. For example, military and civilian institutions in the government often restrict access to information those who need that information. The first formal work in the computer security

was motivation of the military's attempt to implement controls to enforce a "need to know" principle. This principle also applies to industrial firms, which keep their proprietary designs secure their competitors try to steal the designs. As a further example, all types of institutions keep personnel records secret.

Access control mechanisms support confidentiality. One access control mechanism for preserving confidentiality is cryptography, which scrambles data to make it incomprehensible. A cryptography key controls access to the unscrambled data, but then the cryptographic key itself becomes another datum to be protected.

Example: Enciphering an income tax return will prevent anyone from reading it. If the owner needs to see the return, it must be deciphered. Only the possessor of the cryptographic key can enter it into a deciphering program. However, if someone else can read the key when it is entered into the program, the confidentiality of the tax return has been compromised.

Example: The user of Computer A sends a message to the user of the computer B. Another user C get access to this message, which is not desired, and therefore, defeat the purpose of confidentiality. For an example an email message is send by A to B, which is accessed by C with the permission of both.

Other system-dependent mechanisms can prevent processes from illicitly accessing information. Unlike enciphered data, however, data protected only by these controls can be read when the controls fail or bypassed. Then their advantage is off-set by a corresponding disadvantage. They can protect the secrecy of data more completely than cryptography, but if they fail or evade, the data becomes visible.

Confidentiality also applies to the existence of data, which is sometimes more revealing than the data itself. Access control mechanisms sometimes conceal the mere existence of data; less the existence itself reveal information that should be protected.

Resource hiding is another important aspect of confidentiality. Sites often wish to conceal their configuration as what systems that are using; organization may not wish others to know about specific equipment because it could be used without authorization or in inappropriate ways, and a company renting time from a service provider may not want others to know what resources it is using. Access control mechanisms provide these capabilities as well.

All the mechanisms that enforce confidentiality require supporting services from the system. The assumption is that security services can rely on the kernel, and other agents, to supply correct data. Thus, assumptions and trust underlie confidentiality mechanisms.

Integrity:

To ensure that no changes or errors are introduced in the messages during transmission. Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized changes. Integrity includes data integrity (the content of the information) and origin integrity (the source of the data, often called authentication). The source of the information may bear on its accuracy and creditability and on the trust that people place in the information. This illustrates the principle that the aspect of integrity known as creditability is central to the proper functioning of the system.

Integrity mechanisms fall into two classes: prevention mechanisms and detection mechanisms. Prevention mechanisms seek to maintain the integrity of the data by blocking any unauthorized attempts to change the data or any attempt to change the data in unauthorized ways. The distinction between these two types is important. The former occur when a user tries to change the data which has no authority to change. The latter occurs when a user authorized to make certain changes in the data tries to change the data in the other ways.

Adequate authentication and access controls will generally stop the break-in from the outside, but preventing the second type of attempt requires very different control. Detection mechanisms do not try to prevent violations of integrity; they simply report that the data's integrity is no longer trustworthy. Detection mechanisms may analyze system events to detect problems or may analyze the data itself to see if required or expected constraints still hold. The mechanisms may report the actual cause of the integrity violations (a specific part of a file was altered), or they may simply report that the file is now corrupt.

Working with integrity is very different from working with confidentiality. With confidentiality, the data is either compromised or it is not, but integrity includes both the correctness and the trustworthiness of the data. The origin of the data, how well the data is protected before it arrived at the current machine, and how well the data is protected on the current machine all affect the integrity of the data. Thus, evaluating integrity is often very difficult, because it relies on assumptions about the source of the data and about trust in that source-two underpinning of security that are often overlooked.

Non-repudiation:

To ensure that an entity cannot later deny the origin and receipt and contents of the communication

There should be an appropriate institutional arrangement for key management and authentication. This is normally done through Certification Agencies. For the banking and financial sectors' the RBI should appoint a suitable agency/institution as the Certificate Agency. There should also be an institutional arrangement for appropriate assessment of participants of the financial network in terms of their credit-worthiness, financial soundness, etc. These assessments will provide valuable input to the banking and financial sector.

Initially the Indian Financial Network (INFINET) will be a Closed Used Group (CUG) network, but in due course this network will have to be connected to public networks like the Society for World-wide Interbank Financial Telecommunication (SWIFT) etc. It is essential to look at the possibility of having firewall implementations and they need to meet the following criteria:

- All in and out traffic must pass through the firewall. The firewall should check and authorize the traffic. The firewall in itself should be immune to penetration.
- Implementation of firewalls can be done using packet filtering routers, application and circuit level gateways and also network translation devices.
- State full multilayer inspection gateways combine the advantages of the above and also give a better performance, flexibility and security. This environment can handle all kinds of applications, namely, Transmission - Control Protocol (TCP), User Datagram Protocol (UDP), Remote Procedure Call (RCP), Internet Control Message Protocol (ICPMP) etc. New applications can be added easily and this environment is totally transparent to end-users.
- Firewalls are used to implement access control security as well as to provide for user authentication and to ensure data integrity by using encryption. It is important that the banks have their own security policy and then design security solutions accordingly. Regular reviews of security Policies and their implementation are also important. Highly secured (e.g., funds related), secured, non-secured messages should be clearly demarcated in the security policy. Banks are, therefore, advised to have dedicated groups with enough competence and capability. Since security is the prime concern for the banking and financial sector, continuous research should be carried out as is done in the internet community. Institution like IDRBT should have collaborative arrangements with national and international agencies for carrying out research in this field. Such

Institutions could develop Tiger teams (hackers) and the banks can engage the team to test and determine the strength of the firewall implementation.

Mobile information security

Modern day smart phones offer wireless internet connectivity. Cyber security has been an important topic in the today's scenario. In fact, a recent study by the Center for Strategic and International Studies wrote, "Cyber security is among the most serious economic and national security challenges we face in the twenty-first century". For a company to achieve effective mobile commerce security and ultimately consumer trust the security mechanisms will constitute as a security risk. The mechanisms are:

Authorization – It means ensuring authorized uses of systems and performance of business functions by authorized users only.

Authentication – Authentication is establishing that parties to an electronic transaction or communication are who they claim they are.

Integrity- Ensuring that data on the host system or in transmission are not created, intercepted, modified or deleted illicitly.

Confidentiality- Warranting that data are only revealed to parties who have a legitimate need to know it or have access to it.

Availability - Ensuring that legitimate access to information and services is provided. It should be available every time when it is required.

Non-repudiation - If a party to some transaction or communication later denies that it has ever happened, some mechanism is in place to facilitate dispute resolution.

Privacy - Ensuring that customers' personal data collected from their electronic transactions are protected from indecent and/or unauthorized disclosure.

Major issues in cyber space

Malware is getting stealthier, more targeted, multi-faceted and extremely difficult to analyze and defeat even by the experts in the security field. Organized crime is fast growing and targeting the exponential growth of on line identities and financial transactions. There is increasing evidence of espionage, targeted attacks and lack of traceability in the cyber world as state and non-state actors are compromising, stealing, changing or destroying information and therefore potentially causing risk to national security, economic growth, public safety and competitiveness.

Major issues related to cyber space:

1. Developments of cyber space pave the way for cyber crimes.
2. In some cases, identification of the user is not possible.
3. E-mail address has digital identity, but it does not show the reliable identity.
4. Passwords are used as identity but are shared easily.
5. Internet protocol (IP) addresses serve as an address for a computer. But it does not identify the user of a computer.

The Need for an Indian Cyber Law

In today's techno savvy environment, the world is becoming more and more digitally sophisticated and so are the crimes. Internet was initially developed as a Research and information sharing tool and was in an unregulated manner. As the time passed by it became more transactional with e-business, e-commerce, E-governance and e-procurement etc. Today adversaries are producing, selling and distributing malicious code with ease, maximizing their gains and exploiting the fact that attribution is a challenge. Malware is getting stealthier, more targeted, multi-faceted and extremely difficult to analyze and defeat even by the experts in the security field. Organized crime is fast growing and targeting the exponential growth of on line

identities and financial transactions. There is increasing evidence of espionage, targeted attacks and lack of traceability in the cyber world as state and non-state actors are compromising, stealing, changing or destroying information and therefore potentially causing risk to national security, economic growth, public safety and competitiveness. All legal issues related to internet crime are dealt with through cyber laws. In today's highly digitalized world, almost everyone is affected by cyber law. As the number of internet users is on the rise, the need for cyber laws and their application has also gathered great Momentum. For example

- Almost all companies extensively depend upon their computer networks and keep their valuable data in electronic form.
- Government forms including income tax returns, company law forms etc are now filled in electronic format.
- Consumers are increasingly using credit cards for shopping.
- Most people are using email, cell phones and SMS messages for communication.
- Even in "non-cyber crime" cases, important evidence is found in computers / cell phones e.g. in cases of divorce, murder, kidnapping, tax evasion, organized crime, terrorist operations, counterfeit currency etc.
- Cyber crime cases such as online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, pornography etc are becoming common.
- Digital signatures and e-contracts are fast replacing conventional methods of transacting business.
- Almost all transactions in shares are in demat form.

Technology is never a disputed issue but for whom and at what cost has been the issue in the ambit of governance. The cyber revolution holds the promise of quickly reaching the masses as opposed to the earlier technologies, which had a trickledown effect. Such a promise and potential can only be realized with an appropriate legal regime based on a given socio-economic metrics

Cyber law-Governance

Cyber law governs the four major parts. They are

1. Cyber crimes
2. Electronic signature
3. Intellectual property and
4. Data privacy

1. Cyber crimes

Cyber crimes are illegal activities done with the use of network linked technology. Fraudulent people target the computers to attack the confidentiality and the information of the victims. They use computers as a tool for cheating, gambling, illegal copying etc. Some of the people commit a crime by downloading unauthorized software, contraband, stealing the trade secrets, accessing the website in an unauthorized way. So it is more important to govern the activities which are involved in cyber space.

2. Electronic signature

To make the electronic document genuine and legally acceptable, digital signature is necessary. It authenticates the person who signs and the message as genuine and honest.

With the advancement in technology, the use of the internet for business transactions has also increased. Most of the transactions require you to provide important information about yourself. This information is processed to complete the transactions. However, the business organizations need to verify that the information that you provide is correct and authentic. To

ensure this, a digital signature is used by users. A digital signature is similar to a handwritten signature.

Functions of digital signature:

1. To authenticate the identity of the user of the signature.
2. To ensure that the contents of the signed documents cannot be changed or distorted.
3. To ensure non-repudiation that means the user of the signature cannot deny sending the information that was digitally signed.

   Digital signature provides improved security, which increases the confidence of the user of digital information exchange.

Handwritten signature cannot be stolen but can be easily forged. However, digital signature is impossible to forge. The only problem with the digital signature is that they can be stolen if care is not taken. Therefore, digital signature should be kept confidentially.

To make the electronic document genuine and legally acceptable, digital signature is necessary. It authenticates the person who signs and the message as genuine and honest. Unlike handwritten signature, you can see multiple digital signatures in different ways for various purposes. You can see the same signature whenever you have to authenticate a document. However, you can have a number of digital signatures depending upon the requirement and purpose.

Digital signatures are created using public key cryptography. When a user implements a digital signature, two keys are generated. One of these keys is a private key that is kept secret. The other is a public key, which is available to all. The private key is used to generate a digital signature that is used to sign an electronic document.

Consider that you want to digitally sign an electronic document. First, a special function in the encryption software automatically produces a unique summary of the document that has to be encrypted. This summary is called a message digest. Then, the message digest is encrypted with your private key to produce the digital signature.

After the signature is created, you send the original document and signature to the recipient who uses your public key to verify the signature. The public key does not verify the signature even if there is a minor alteration to the file. This is because the alteration results in a different message digest. This ensures that the message that you send is not modified by anyone. The signature is also not be verified if the private and public keys do not modified by anyone. The signature is also not be verified if the private and public keys do not match.

A digital signature ensures that the receiver does not accept an altered message. Digital signature also ensures non-repudiation. Non-repudiation is achieved through cryptography methods. If an individual uses a digital signature, the signature prevents the individual from denying having performed a particular action related to the digitally signed data. Digital signature provides evidence to a third party that an action has occurred. Digital signatures can be specifically used to provide evidence in the non-repudiation of approval, submission and receipt during online transaction.

If person conducts transaction by using digital signature, it implies that the person has used the private key. This private key is assumed to be in safe custody of the holder and is inaccessible to the others. In addition it is not possible to forge the digital signature. Therefore only the sender of the message could have generated the message that results in a transaction.

3. Data privacy

Data privacy is very much required for an individual corporation and government. Normally password and encryption technology are used as a security measure to protect data in cyber space. In spite of this, password is stolen and data is extracted. The password is stolen by way of matching the dictionary words with the password. So everyone must be caution while framing the password for data privacy. With encryption, the data can be securely transmitted via internet. Encryption can protect the data at the simplest level by preventing other people from reading it.

4. Intellectual property

Intellectual property refers to intangible or non-physical goods. It is protected by copyright for written works, patents for inventions and trade marks for brands, names and logo. Intellectual property relating to computer and other electronic means are legally covered under cyber law.

e-Mudhra

e-Mudhra, a Certification Authority (CA), offers secure digital signatures through various options tailored to suit individual as well as organizational needs.

A Digital Signature Certificate (DSC) is a secure digital key that certifies the identity of the holder, issued by a Certifying Authority (CA). It typically contains your identity (name, email, country, APNIC account name and your public key). Digital Certificates use Public Key Infrastructure meaning data that has been digitally signed or encrypted by a private key can only be decrypted by its corresponding public key. A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web.Digital Signature Certificates (DSC) along with digital signatures for specific needs such as Income Tax filing, MCA, e-tendering, e-procurement and Foreign Trade.

As e-filing is made compulsory in ROC, every director / signing authority needs to have their Digital Signature Certificate. Its now mandatory to obtain PAN Encryption Digital Signature Certificate for any person who is required to sign manual documents and returns filed with ROC as per MCA21. Also an Individual is required to obtain DSC with PAN Encryption for e-filing his return with Income Tax, India.

Digital Signature Certificate is the upgraded version of previous Digital Signature Certificate. By Using This Certificate You can Participate/Bid in Any Kind of On-line Tenders/Auction across India. To participate in the e-tendering process, every vendor is required to use a latest version of Digital Signatures Certificate.

Data Security:

In any electronic transactions data security is a must. Data security means protection of database from hackers by using security measures. Unauthorized access of data or destruction of data may lead to numerous problems for larger corporations and also for the personal home users. Data security is an important area of concern for every business owner, consumer and for the individual.

Fundamentals of data security requirements

The following are the basic security standards which technology must ensure:

I. Confidentiality
II. Integrity
III. Availability

Confidentiality

A secured system ensures the confidentiality of data. It allows individuals to see only the data which they are supposed to see. Confidentiality has several aspects, which are discussed below

a. Privacy of communications
b. Storage of sensitive data safely
c. Authenticated users
d. Access control

Privacy of communication

Privacy is a very broad concept. For the individual, it involves the ability to control the spread of confidential information. In the business world, privacy may involve the ability to keep trade secrets, proprietary information about products and processes, business strategies, as well as marketing and sales plans. For Governments, privacy involves the ability to keep secrets that affect the country's interests.

Data Protection has been defined to include-

- The legal safeguards of people's rights to see what information may be held about them in a computer database, and

- The protection from theft, destruction, or damages of software (programs) and data held in a computer's memory. The second type of data protection is also often called data security.

Examples of the former are Government departments and commercial companies that hold personal data in computers. For example, a company may have a computer database listing the names and addresses of the customers. At ax office may have a similar computerized list of everyone who pays income tax. Some countries have laws giving various rights to people listed in such database. In the UK, the 'Data Protection Act 1984' safeguards the individual's right to see his or her database entries, alter inaccuracies, or in some cases have it deleted. According to this Act, organization holding computerized personal data must register with the 'Data Protection Registrar'. Organizations registered with the Data Protection Registrar must show any individual whatever information they hold on that person, except in a few instances. Any organization that ought to have registered, but has not registered, is committing a criminal offence. Similarly laws operate in other countries also, especially in Europe.

As far as the latter category is concerned, a technologically advanced India remains handicapped for want of legal support in implementing many of the technological innovations. The absence of law relating to digital signature and encryption prevents our company from implementing Electronic Fund Transfer (EFT) in a big way, apart from depriving the country of the benefits of E-Commerce. Apart from the above, the absence of law and legal deterrents relating to computer crime emboldens many a computer criminal in the country to indulge in computer crime. The absence of the provisions enabling electronic data as 'admissible evidence' in the courts has put our country decades back to other nations.

Precautionary Measures

Data Protection has been defined to include-

- The legal safeguards of people's rights to see what information may be held about them in a computer database, and

- The protection from theft, destruction, or damages of software (programs) and data held in a computer's memory. The second type of data protection is also often called data security.

Examples of the former are Government departments and commercial companies that hold personal data in computers. For example, a company may have a computer database listing the names and addresses of the customers. At ax office may have a similar computerized list of everyone who pays income tax. Some countries have laws giving various rights to people listed in such database. In the UK, the 'Data Protection Act 1984' safeguards the individual's right to see his or her database entries, alter inaccuracies, or in some cases have it deleted. According to this Act, organization holding computerized personal data must register with the 'Data Protection Registrar'. Organizations registered with the Data Protection Registrar must show any individual whatever information they hold on that person, except in a few instances. Any organization that ought to have registered, but has not registered, is committing a criminal offence. Similarly laws operate in other countries also, especially in Europe.

As far as the latter category is concerned, a technologically advanced India remains handicapped for want of legal support in implementing many of the technological innovations. The absence of law relating to digital signature and encryption prevents our company from implementing Electronic Fund Transfer (EFT) in a big way, apart from depriving the country of the benefits of E-Commerce. Apart from the above, the absence of law and legal deterrents relating to computer crime emboldens many a computer criminal in the country to indulge in computer crime. The absence of the provisions enabling electronic data as 'admissible evidence' in the courts has put our country decades back to other nations.

Cyber Security

Introduction in Cyber Security

Cyber Security, also referred to as information technology security, applied to computing devices such as computers and smart phones, as well as to both private and public computer networks, including the whole Internet. It focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.

Cyber Security is the process of applying security measures to ensure confidentiality, integrity, and availability of data. Cyber Security attempts to assure the protection of assets, which includes data, desktops, servers, buildings, and most importantly, humans. The goal of cyber security is to protect data.

Governments, Financial institutions, Hospitals and other businesses collect the process and store a great deal of confidential information on computers and transmit that data across networks to other computers. With the growing volume and sophistication of cyber attacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security.

Fig – 2.1 Cyber security

Risk in Cyber Security

The Exponential growth of the Internet, Wireless media applications and services pose new security challenges. Security is a complex system and must be considered at all points and for every user. Organizations need systematic approach for security management that addresses security consistently at entry level. They need systems that support optimal allocation of limited security resources on the basis of predicted risk rather than perceived vulnerabilities. Cyber Security plans call for more specific requirements for computer and network security as well as emphasis on the availability of commercial automated reporting mechanisms for security assessments and threat management.

Security requirement specification and risk analysis collects information regarding assets of the organization that need to be protected. Based on risk analysis report, several security policies are generated. Several tests are carried out to test the effectiveness of the security, functionality of the access control and existence of vulnerabilities.

Cyber Security Risk Avoidance Factors

Access Control

It refers to the rules and deployment mechanisms which control access to information systems and physical access to premises.

Access Control List

An access control list (ACL) is a file which a computer's operating system uses to determine users individual access rights and privileges to files on a system.

Anti Virus Program

Software designed to detect and potentially eliminate viruses before they have had a chance to cause destruction within the system, as well as repairing files which have already been infected by virus activity.

Application Service Provider

An Application Service Provider rents software to users and provides access over the Internet.

Audit log

Computer files containing details of records, which may be used in the event of system recovery being required.

Biometric access controls

Security access control systems which authenticate users by means of physical characteristics e.g.: face, fingerprints and voice.

Denial of service

Denial of service (Dos) is an action against a service provider over the internet whereby a client is denied the level of service expected. DoS attacks do not usually have theft or corruption of data as their primary motive.

Security for electronic transactions (SET)

SET was originally supported by companies such as MasterCard visa provides a means for enabling secure transactions between purchaser, merchant and bank.

Hackers

Hacking in computers is the unauthorized access and use of networked computer systems. Hackers can be outsiders or company members. They can use the Internet to steal or damage the data.

Some hackers who commits only electronic breaking and entering; they can access the system and reads some files but neither steals nor damages anything. Hackers can monitor mails, file transfers to extract passwords and also steal network files. A hacker may also use remote

services that allow one computer on network to execute programs on another computer to gain privileged access within a network.

Telnet an Internet tool for interactive use of remote computers, can help hackers discover information and to plan other attacks. Hackers have used Telnet to access a computer mail port, to monitor the messages, passwords and other information about user accounts and network resources. These are the crimes hackers commit on the network.

Types of Hackers

The different types of Hackers are

- ✓ **White Hat Hackers**
- ✓ **Black Hat Hackers**
- ✓ **Blue Hat Hackers**
- ✓ **Spy Hackers**

White Hat Hackers

White hat hackers are hackers who perform hacking for legitimate reasons. These are the good guys, computer security experts who specialize in penetration testing and other methodologies to ensure that a company's information systems are secure. These IT security professionals rely on a constantly evolving arsenal of technology to battle hackers.

Black Hat Hackers

These are the bad guys, who are typically referred to as just plain hackers. The term is often used specifically for hackers who break into networks or computers, or create computer viruses. Black hat hackers continue to technologically outpace white hats. They often manage to find the path of least resistance, whether due to human error or laziness, or with a new type of attack. Hacking purists often use the term "crackers" to refer to black hat hackers. Black hats' motivation is generally to get paid.

Blue Hat Hackers

A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch, looking for exploits so they can be closed. Microsoft also uses the term Blue hat to represent a series of security briefing events

Spy Hackers

Corporations hire hackers to infiltrate the competition and steal trade secrets. They may hack in from the outside or gain employment in order to act as a mole. Spy hackers may use similar tactics as hacktivists, but their only agenda is to serve their client's goals and get paid.

Common Hacking Tactics

Sniffer

Sniffer is the programs that secretly search individual packets of data as they pass through the internet, capturing the passwords and contents. It is also called as spoofer. It is a standalone program to intercept and analyze certain data. For example a sniffer can intercept and analyze network traffic and catch certain data, for example passwords. Trojans sometimes use sniffing capabilities to steal passwords and user information from infected computers. There also exist a lot of commercial and free sniffers. They can be used to analyze network traffic for performance, security issues and faults.

Sniffer is a Network analyzing tool. Network analyzing tools are used to monitor the traffic conversations that occur across the network. Often the information obtained from a sniffer can be used to figure out exactly how devices are communicating. But the use of a sniffer is not

limited to troubleshooting, it can also be used to help train, design and operate devices on a network.

Spoofing

Spoofing is the process of faking the websites or mails to trick users into passing along critical information like credit card numbers or passwords.

A spoofing attack is user on a network; in order to launch attacks against network hosts, steal data, spread malware etc. Many of the protocols do not provide mechanisms for authenticating the source or destination of a message. They are thus vulnerable to spoofing attacks when extra precautions are not taken by applications to verify the identity of the sending or receiving host. Spoofing attacks which take advantage of protocols may be mitigated with the use of firewalls capable of deep packet inspection or by taking measures to verify the identity of the sender or recipient of a message.

Malicious Applets

A malicious applet is any applet that attacks the local system of a Web surfer. Malicious applets are written by researchers, crackers, and Net miscreants to annoy and damage Java users. They can even seriously damage a Java user's machine. These are tiny programs, written in the popular java computer language, that misuse your computer resources, modify files on the hard disk, send fake mails or steal passwords. Any applet that performs an action against the will of the user who invoked it should be considered malicious.

These are tiny programs, sometimes written in the popular java computer language, that misuse your computer resources, modify files on the hard disk, send fake mails or steal passwords.

Logic bomb

A logic bomb is a piece of programming code buried within another programme, designed to perform some malicious act. It is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting important files of a company or organization, which will lead problems to the organization.

Software that is inherently malicious, such as logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates, such as Wednesday the 12th or Independence Day. Viruses that activate on certain dates are often called "Time bombs".

Threat

A threat is anything that can disrupt the operation, functioning, integrity, or availability of a network or system.

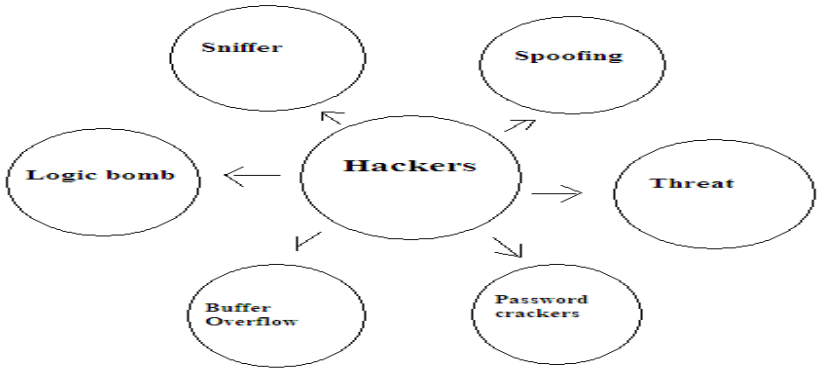


Fig – 2.2 Hackers

Buffer Overflow

It is a technique for crashing or gaining control of a computer by sending too much data to the buffer in a computer's memory.

War Dialing

These are the programs that automatically dial thousands of telephone numbers in such a way through a modem connection.

Password Crackers

It is the software that can guess passwords. Password attacks can be implemented using several different methods like brute force attacks, Trojan horse programmers. IP spoofing can yield user accounts and passwords. Password attacks usually refer to repeated attempts to identify a user password or account.

Attackers

An intentional violation of a security objective is called an attack. Attacks may either be initiated by outsiders or insiders. Targeted attacks intend to harm a specific communication system. Untargeted attacks victimise any vulnerable system by discover. Targeted attacks are typically preceded by a phase of gathering information about the target, e.g. using online and offline available references, as well as dedicated tools for discovering vulnerable systems on a network.

Types of attacks:

Breaking into a system

Through violation of the authentication and access control objectives, the attackers obtain the ability to control aspects of the behaviour of the communication system including the ability to overcome confidentiality and integrity objectives.

Virus

A virus based attack manipulates a legitimate user to bypass authentication and access control mechanisms in order to execute the malicious code injected by the attacker. Virus attacks are often untargeted and spread among vulnerable systems and users. Virus attacks often directly or indirectly decrease the availability of infected systems by consuming excessive amounts of processing power or network bandwidth.

A virus is a computer program that attaches itself to another legitimate program and causes damage to the computer system or to the network. During its life time, a virus goes through **four phases**, they are:

Dormant phase: here, the virus is ideal. It get activated based on certain action or event (e.g. the user typing a certain key or certain date or time is reached, etc). This is an optional phase.

Propagation phase: in this phase, a virus copies itself and each copy starts creating more copies of self, thus propagating the virus.

Triggering phase: A dormant virus moves into this phase when the action/event for which it was waiting is initiated.

Execution phase: This is the actual work of the virus, which could be harmless (display some message on the screen) or destructive (delete a file on the disk).

Viruses can be classified into following categories:

Parasitic Virus: This is the most common form of viruses. Such a virus attaches itself to executable files and keeps replicating. Whenever the infected file is executed, the virus looks for other executable files to attach itself and spread.

Memory-Resident Virus: This type of virus first attaches itself to an area of the main memory and then infects every executable program that is executed.

Boot sector virus: This type of virus infects the master boot record of the disks and spreads on the disk when the operating system starts booting the computer.

Stealth virus: This virus has intelligence built in, which prevents anti-virus software program from detecting it.

Polymorphic Virus: A virus that keeps changing its signature (i.e. Identity) on every execution, making it very difficult to detect.

Metamorphic Virus: In addition to changing its signature like a polymorphic virus, this type of virus keeps rewriting itself every time, making its detection even harder.

There is another popular category of viruses called as the macro virus. This virus affects specific application software, such as Microsoft Word or Microsoft Excel. These viruses affect the documents created by the users and spread quit easily since such documents are very commonly exchanged over email. There is a feature called as macro these application software programs, which allows the user to write small useful utility programs within the documents. Viruses attack these macros and hence the name macro virus.

Trojan

A Trojan is a virus where the malicious functionally is hidden behind functionality that is desired and used by the user. Trojans are typically employed to circumvent confidentiality or access control objectives.

Worm

A worm is malicious code whose propagation mechanisms rely on automatic exploration and exploitation of vulnerabilities in the targeted system, without involvement of any user. Worm infections are untargeted and usually create availability problems for the affected system or even the Internet as a whole.

Cracking

The term “cracking” means trying to get into computer systems in order to steal, corrupt, or illegitimately view data. The popular press refers to such activities as hacking, but hackers see themselves as expert, elite programmers and maintain that such illegitimate activity should be called “cracking.”

The term cracker was coined by Richard Stallman. Crackers are unauthorized users who attempt to obtain unauthorized access to remote systems. The nature of these attacks has changed substantially over the last few years. Several years ago crackers sat at terminal entering commands, waiting to see what would happen, and then entering commands. Today most cracking attacks are automated and take of attack is sometimes called an asymmetric attack.

Data recovery

Data recovery is the process of handling the data; through the data is damaged, failed, corrupted or cannot accessible from secondary storage media then it cannot be accessed normally. The data are being kept in storage media such as internal or external hard disk drives, pen drive, storage tapes, CDs, DVDs etc. Recovery is needed due to physical damage to the storage device or logical damage to the file system that prevents it from being mounted by the host operating system (OS).

The most common data recovery scenario involves an operating system failure, accidental damage etc; in such case copy all wanted files to another disk. This can be easily done by using a CD or pen drives. In order to move the files from the system disk to the backup media file manager or optical disc authoring software is used.

In case of hard disk failure, the data cannot be easily read. The solutions are repairing the file system, hard disk recovery techniques to recover the corrupted data, hardware-software based recovery of damaged service areas to hardware replacement on a physically damaged disk.

If the Files erased, then the contents of deleted files are not removed immediately from the drive; instead, references to them in the directory structure are removed, and the space they occupy is made available for later overwriting. For the end users, deleted files are not discoverable through a standard file manager, but that data still technically exists on the drive.

In the meantime, the original file contents remain, often in a number of disconnected fragments, and may be recoverable. The Data recovery process is also used in forensic applications.

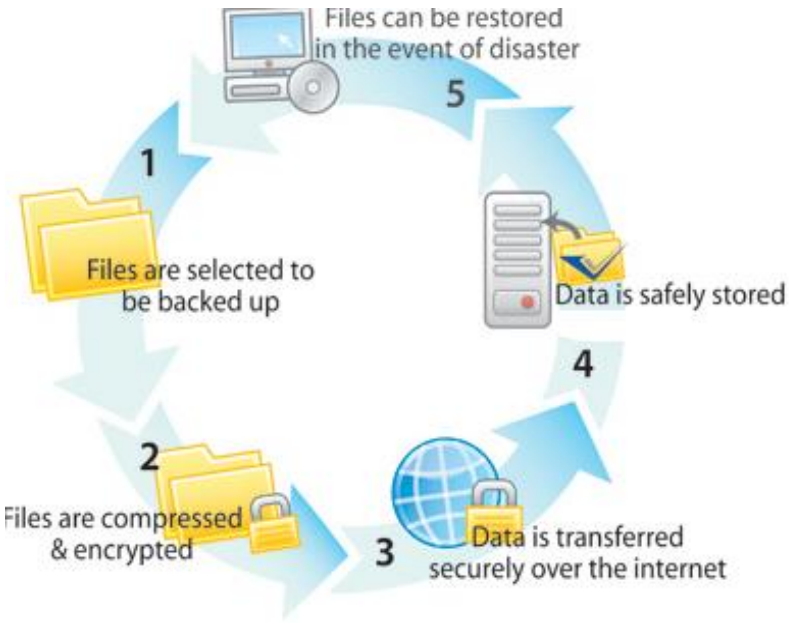


Fig – 2.3 Data Recovery

Types of Data Access Methodologies

Sequential Access

It is a simple access method. All the records are kept in some sequence such as numerical order. Records in this type of file are located one after another according to the given order. The information in a file is accessed sequentially one record after another. Sequential access is based on the tape model that is inherently a sequential access device. Sequential access is best suited where most of the records in a file are to be processed. For example, transaction files.

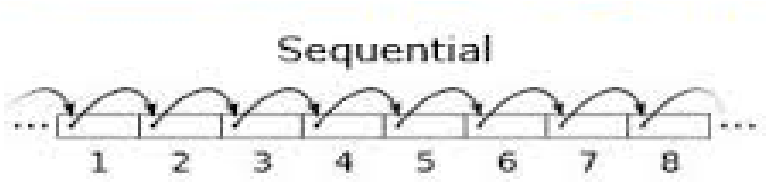


Fig – 2.4 Sequential Access

Direct Access

Direct access file uses a physical medium and programming, which helps in the storage and retrieval of specific records. These files are the heart of DBMS and most of today's file storage technology. Sometimes it is not necessary to process every record in a file. It may not be necessary to process records in the order in which they are present. Most common device for storing direct access files is magnetic disk.

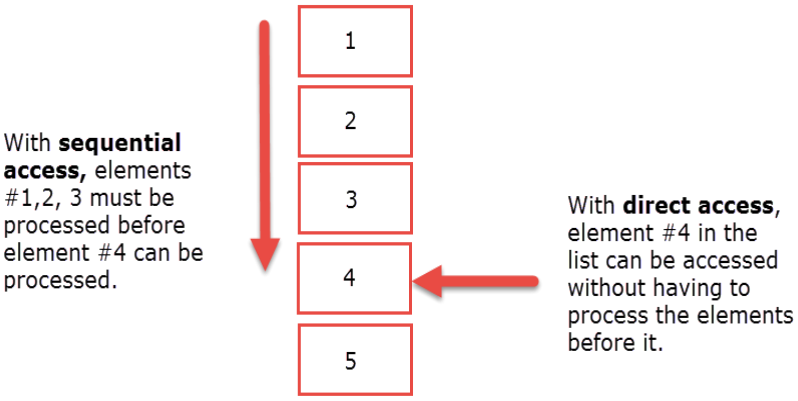


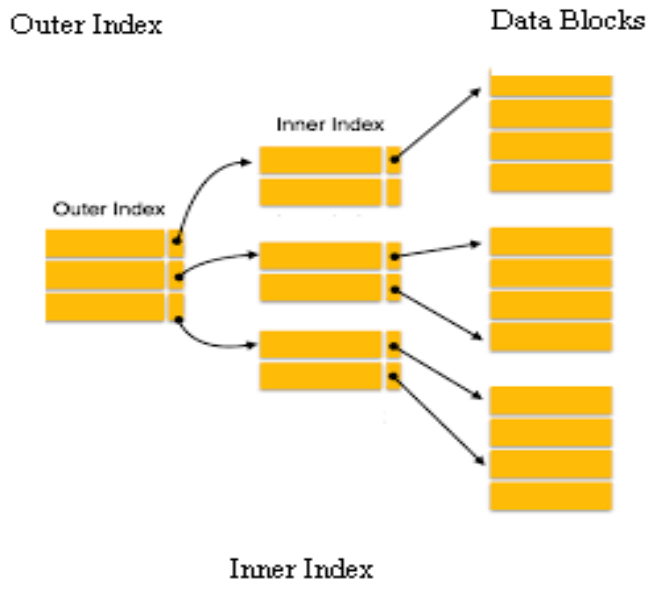
Fig – 2.5 Direct Access

Information present in a record can be accessed only if some key value in that record is known. In all such cases, direct access is used. A file is a collection of physical blocks, and so the records in any block can be accessed. For example, master files.

Databases are of this type since they allow query processing that involves immediate access to large amounts of information. Not all operating systems support direct access files. Usually files are to be defined as sequential or direct at the time of creation and accessed accordingly later. All reservation systems fall into this category.

Indexed Sequential Access

This access method is a slight modification of the direct access method. It is a combination of both the sequential access as well as direct access. The main concept is to access a file direct first and then sequentially from that point onwards. This access method involves maintaining an index. The index is a pointer to a block. To access a record in a file, a direct access of the index is made. The information obtained from this access is used to access the file. For example, the direct access to a file will give the block address and within the block the record is accessed sequentially. Sometimes indexes may be big. So hierarchies of indexes are built in which one direct access of an index leads to info to access another index directly and so on till the actual file is accessed sequentially for the particular record. The main advantage in this type of access is that both direct and sequential access of files is possible.



Methodology that helps in Remote Data recovery are:

Logical recovery of files & partition

After the drive has been ready to use, it is possible the retrieve the lost data. If the drive has failed logically, there are a number of reasons for that. User can repair the files in order to read the file system's data structure and retrieve stored data.

Repair the damaged files can be retrieved

Data loss or damage may occur when, for example, a file is written to a sector on the drive that has been damaged. Corrupted documents can be recovered by several software methods or by manually reconstructing the document using a hex editor.

Recover Swap File

Swap file is a file stored on the computer hard drive that is used as a temporary location to store information that is not currently being used by the computer RAM. By using a swap file a computer has the ability to use more memory than what is physically installed in the computer.

It is useful technique that enables a computer to execute programs and manipulate files larger than main memory. The operating system copies as much data as possible into main memory, and leaves the rest on the disk. The least recently used files in RAM can be "swapped out" to hard disk until they are needed. New files can be "swapped in" to RAM. In larger operating systems the units that are moved are called pages and the swapping is called paging.

Swap files are used in operating systems like Windows 7 and Windows Server 2008, as virtual memory is a cheaper alternative to magnetic media. A typical swap file is equal to or larger than the system's total installed physical memory. Although swap files provide additional system memory, the data stored in swap files is typically less active and idle. The swap files can be corrupted due to raw partition, virus attacks or system crash. User can get back the corrupted files by using the recovery tools. These recovery tools helps in the maintenance of swap file data in a secured way.

Recover Temporary Files

Deleted files are inaccessible. We can often recover them completely with professional data recovery tools. Data recovery software is designed to locate any recoverable data and providing it in a proper format. The best data recovery applications provide a preview of recovered files, filtered and searchable results and easy file restoration

File recovery programs can be used to save files of any type or size, from pictures, music and videos to documents and spreadsheets. Data recovery software can locate and restore emails,

executables and compressed files. The best file recovery software can even maintain the folder organization of your files, and it may be able to recover a complete partition or drive.

Data recovery in Cache Files

A cache is a place to store something temporarily in a computing environment. The active data is often cached to shorten data access times, reduce latency and improve input/output. Because almost all application workload is dependent upon I/O operations, caching is used to improve application performance.

The web browsers such as Internet Explorer, Firefox and Chrome use a browser cache to improve performance for frequently accessed web pages. When you visit a webpage, browser requests are stored on computing storage in the browser's cache. If you click "back" and return to that page, your browser can retrieve most of the files it needs from cache instead of requesting they all be sent again. This approach is called read cache. It is much faster for your browser to read data from the browser cache than to have to re-read the files from the web page.

Types of cache

Write-around cache

It allows write operations to be written to storage, skipping the cache altogether. This keeps the cache from becoming flooded when large amounts of write I/O occur. The disadvantage is that data is not cached unless it is read from storage. As such, the initial read operation will be comparatively slow because the data has not yet been cached.

Write-through cache

It writes data to both the cache and storage. The advantage to this approach is that newly written data is always cached, thereby allowing the data to be read quickly. A drawback is that write operations are not considered to be complete until the data is written to both the cache and primary storage. This causes write-through caching to introduce latency into write operations.

Write-back cache

It is similar to write-through caching in that all write operations are directed to the cache. The difference is that once the data is cached, the write operation is considered complete. The data is later copied from the cache to storage. In this approach, there is low latency for both read and write operations. The disadvantage is that, depending on the caching mechanism used, the data may be vulnerable to loss until it is committed to storage.

Steps to retrieve the cache files from different browsers:

Retrieve temporary Internet files from Internet Explorer versions 7 and 8.

- ✓ Access and open Internet Explorer through your Start menu or by clicking on the icon directly from your desktop. Click on Tools, then on Internet Options. Click on the General tab and then click on Settings under the Browsing History section. In Settings, click on View Files to retrieve and view your temporary Internet files.

Retrieve temporary Internet files from Internet Explorer 6.

- ✓ Access and open Internet Explorer through your Start menu or by clicking on the icon directly from your desktop. Click on Tools, then on Internet Options. Click on the General tab and then click on Settings under the Temporary Internet Files section. In Settings, click on View Files to retrieve and view your temporary Internet files

Retrieve temporary Internet files from Google Chrome.

- ✓ Type "about:cache" directly into the address bar of Google Chrome. Your temporary Internet files, or cache content, will then be displayed in the browser window. Depending on how full your cache is, the data may take a few moments to display.

Authentication

Authentication is how one proves that they are who they say they are. When you claim to be Jane Smith by logging into a computer system as "jsmith", it's most likely going to ask you for a password. You've claimed to be that person by entering the name into the username field (that's the identification part), but now you have to prove that you are really that person. Most systems use a password for this, which is based on "something you know", i.e. a secret between you and the system.

Another form of authentication is presenting something you *have*, such as a driver's license, an RSA token, or a smart card. You can also authenticate via something you *are*. This is the foundation for biometrics. When you do this, you first identify yourself and then submit a thumb print, a retina scan, or another form of bio-based authentication.

Once you've successfully authenticated, you have now done two things: you've claimed to be someone, and you've proven that you are that person. The only thing that's left is for the system to determine what you're allowed to do.

Authentication Control

Authentication or identification is the first step in any access control solution. It is the process of identifying the user to verify whether he/she is what he/she claims to be. Normally, identification is done with the help of information that is known to everyone (i.e., user name or user ID) and some personal information known only to the subject (i.e. password). Faced with the threat of identity theft and increasing consequences associated with failing to secure information, enterprises are increasingly looking for stronger forms of authentication to enhance their overall security capabilities. At the same time,enterprises and governments need to take into account other important considerations such as usability, total cost of deployment and maintenance, and integration with existing security solution offerings. Usernames and passwords are the most common authentication techniques. But most organizations do not depend on user name authentication alone since username and passwords are an authentication solution for low-value transactions and for accessing non-sensitive information over the network. Also, experience has shown that usernames and passwords provide relatively weak authentication because they can often be guessed or stolen. They are often difficult to deploy because each application may implement its own scheme, adding to both development cost and user complexity. Also, it is very difficult to maintain and reset the password. Determining the appropriate level of authentication that meets your budget requirements is essential when implementing your secure identity management solution. It is very crucial to identify the appropriate authentication technique depending upon the nature of the business and sensitivity of the information. One has to consider various authentication methods and their pros and cons. The means of authentication are often discussed in terms of "factors" of proof, such as:

- Something you know to prove your identity (e.g., a PIN)
- Something you have to prove your identity (e.g., a smart card)
- Something you are to prove your identity (e.g., a fingerprint)

A good authentication technique contains at least two of the above methods. In a client server environment, strong

Authentication is a combination of server and client authentication:

- Server authentication is when the server proves its identity to the client.
- Client authentication is when clients prove their identity to the server.

There are various authentication techniques that organizations can choose from. A quick discussion on some of these techniques follows:

1. User Password Authentication

It is the most common form of providing identification. When user accesses the resource, access control framework asks for the user name password provided to the user. The credentials are validated against the one stored in the system's repository.

2. Windows user based authentication

Usually, organizations have a list of users stored in the windows active directory. Access control framework should be able to provide authentication for the user of the Primary Domain Controller (PDC).

3. Directory based authentication.

With the rising volume of business over the web, millions of users often try to access the resource simultaneously. In such a scenario, the authentication framework should be able to provide for faster authentication. One such technique is Directory Based Authentication where user credentials are validated against the one which is stored in the LDAP Directory.

4. Certificate based authentication

This is probably one of the strongest authentication techniques where the user is asked to provide his/her digital ID.This digital ID, known as digital certificate, is validated against the trusted authority that issued the digital ID. There are various other parameters that are checked to ensure the identification of the user.

5. Smart card based authentication

This is also used as a second factor authentication. Smart cards are small devices containing co-processors to process cryptographic data.

6. Biometrics

This is the strongest authentication. Known as third factor authentication, it is based on something the user is. It works after the users have provided something they know (User name password) and something they own (either a grid or token) or something they are (retina-scan, thumbprint or thermal scan). It is required in cases where data is top confidential, such as in Military/Defense.

7. Grid based Authentication

This is used as a second factor authentication. It authenticates the user based on something he knows (User name password authentication) and then asks for something he owns (grid card information). Entrust Identity Guard provides such an authentication.

8. Knowledge-based authentication

One of the simplest mechanisms for gaining additional confidence in a user's identity is to challenge the user to provide information that an attacker is unlikely to be able to provide. Based on "shared secrets", this allows for the organization to question the user, when appropriate, to confirm information that is already known about the user through a registration process, or from previous transactions.

9. Machine Authentication

Machine authentication provides validation of the user's computer in a way that secures against a variety of threats in a zero touch fashion, reducing user impact. This is an especially effective method of user authentication where users typically access their accounts from a regular set of machines, allowing for stronger authentication to be performed without any significant impact on the user experience.

10. One Time Password (OTP)

A one time [password is dynamically generated and it is valid only for once. The advantage of one time password is that if an intruder hacks it, he cannot reuse it. There are two types of OTP token generators: synchronous and asychronous. A synchronous token device synchronizes with the authentication service by using time or an event as the core piece of the authentication process. A token device, which is using an asynchronous token generating method, uses a challenge response scheme to authenticate the user.

User names and Passwords

A usernames and password is like the combination for a combination lock or the PIN number for an ATM card. It is a way of proving to a computer that you are who you claim to be. Unfortunately, it can be compromised, just as a combination can be guessed, or all possible combinations attempted, or someone can look over your shoulder as you key in your PIN.

In the past, password guessing was fairly difficult; however, *this is no longer the case*. Hackers have ever-increasing resources and Caltech presents an attractive target, so all accounts on all servers here need to be protected as much as is practical.

The system administrators make it as difficult for hackers as we can to prevent compromise from the server side, but individual account security is dependent on the security of each individual user names and password. This is why it is extremely important for you to use passwords that cannot be guessed.

General Authentication

Password Authentication

Password authentication is the most common method of authentication. It is also the least secure. Password authentication requires the identity to input a user id and a password in order to login. Password length, type of characters used and password duration are password management are now critical concern in enterprises. The ability to easily crack passwords has resulted in high levels of identity theft. As a result, the high risk of passwords means most enterprises now deploy a layered security strategy. A user enters in their id and password for initial login to gain access to only low risk information and applications with other forms of authentication required for higher risk information and applications.

Single Sign On Authentication

Single Sign On (SSO), Reduced Sign On (RSO), or Enterprise Single Sign On (ESSO) is the ability to reduce the number of id's and passwords a user has to remember. In most enterprises, a strong business case can be made to implement single sign on by reducing the number of password related help desk calls. SSO is also the architecture to require stronger forms of authentication for higher risk information and applications. Thus a user may login using their id and password to gain general low risk access to an enterprise. The SSO software enables them to not have to use multiple id's and passwords. However, when the user tries to access more sensitive information and applications, the single sign on software will require the identity to input stronger authentication such as a security token, a digital certificate and/or a biometric.

Lightweight Directory Access Protocol (LDAP) Authentication

Most enterprises use Lightweight Directory Access Protocol (LDAP) directories to handle the centralized authentication. LDAP directories, such as Active Directory, Sun One Directory, Novel e-Directory and other vendors, provide a low cost way of doing fast identity look-ups and authentication as compared to traditional databases. Today it is also common to use virtual LDAP directories to quickly integrate the identity and authentication information contained in one or more databases and/or other LDAP directories. The use of these directories is a critical piece of identity infrastructure that leads to integrating access control.

Access Control Authentication

Access control is the process of granting an identity the ability to physically or electronically access a facility or enterprise. By using LDAP directories and single sign on, many enterprises now integrate their building access control security cards, employee time keeping and other access control accessories into their LDAP identity management system. This reduces the number of identity database silos, since most access control systems use their own identity databases. It also reduces the number of access control accessory systems.

Network Authentication

Network authentication is the process of granting an identity the ability authenticates to a network as well as their authorization. Almost all network authentication systems are now LDAP

based. This includes Microsoft 2000, Linux, Solaris, AIX and HPUX. Many mainframe authentication systems such as RACF are now LDAP enabled.

Biometric Authentication

Biometric authentication s is the process of taking a "piece of you", digitizing it and then using this to authenticate against an identity directory or database. Typical types of biometric authentications include finger scans, digital finger prints, hand scans, retina scans, digital signature scans and others. The use of DNA biometrics is increasingly used in identity verification (the initial identity registration step prior to authentication). Biometrics are commonly used as part of an array of authentication methods used in enterprises.

Strong Authentication

Strong authentication means higher trust of an authentication. For instance, the successful login using a id and password will be given a low level of trust by the enterprise since the id and password are easily obtained by social engineering or password cracking. Stronger authentication methods include digital certificates, security tokens and biometrics. Often, many enterprises use combinations of these including passwords, to place a higher degree of trust for higher risk applications or information access.

Transaction Authentication

Transaction authentication is the process of using other authentication determinants to verify an identity. Often used by financial institutions for higher risk customers or transactions, the transaction software looks at the IP address the user is coming in on, the identity's computer hardware they're using, the time of day, the geo-location the identity is coming from, etc. If the identity successfully logs on using a id and password BUT the other components are not usual, the transaction authentication software may stop a process, flag in real time an administrator and/or ask the user more questions to have more confidence the identity is who they claim to be.

Federated Authentication

Federated authentication is the ability to trust an incoming electronic identity to the enterprise from a trusted partner or website. Protocols enabling this include SAML, Liberty Alliance, Web Services Federation and Shibboleth. When combined with enterprise single sign on systems, the user experience is improved since they no longer have to remember another id and password. Further, enterprise identity authentication standards can be automatically enforced on external identities using the enterprise systems. Identity authentication federation also works in reverse for enterprise employees who access there 401k, benefits, etc, to outside supplier websites. By using federated authentication, the identity doesn't need to remember another separate id and password.

PKI Authentication

Public key infrastructure (PKI) authentication, is another way of doing identity authentication. An identity is given a digital certificate by an Certificate Authority (CA). This is then presented during the authentication process to verify an identity is who they say they are. The level of authentication trust varies for digital certificates depending on the level of identity verification done during the identity registration process as well as the digital certificate revocation process. Digital certificates are becoming more important to authenticate and verify an identity in single sign on systems, document management systems and in web services.

Security Token Authentication

Security token authentication, such as RSA secureID tokens, are used to authenticate an identity (something that you have). During the login process, or if required by a single sign on system for a higher risk application, the identity is required to enter in the numbers appearing on the token screen along with their id. Since the numbers change randomly to the user viewing the screen (but is understood by the central authentication server), there is a higher degree of trust associated with this form of authentication. However, operating costs for security authentication

tokens are higher than the use of password and id since they must be physically issued, replaced and recovered.

Smart Card Authentication

Smart cards are another form of authentication token (something you have). Often they contain a digital certificate as well as additional identity attribute information. Smart card authentication is becoming wide spread. The same smart cards used in an authentication process are now commonly used as well for access control mechanisms to enter physical facilities, buildings, floors and rooms.

Authentication Management

Authentication management is the overall process of managing identities and their authentication mechanisms. In most enterprise authentication management involves authentication policies and processes to manage passwords, digital certificates, security tokens, access control, biometrics, smart cards, LDAP directories, transaction authentication, single sign on and identity authentication federation. Strong business cases can be made to lower authentication costs while at the same time strengthening overall enterprise security.

Wireless Authentication

Authenticating wireless devices is today becoming a main enterprise security issue. Often, the authentication used is very insecure or easily breached. There are however ways to increase reliability that the user is who they claim to be by using multi-factor authentication.

Document Authentication

Formely separate document authentication systems are now becoming intertwined with enterprise identity and authentication mechanisms. Gone are the days of relying upon mostly passwords to authenticate users trying to open document. Formerly separate document authentication systems are now becoming intertwined with enterprise identity and authentication mechanisms. Gone are the days of relying upon mostly passwords to authenticate users trying to open documents.

Outsourcing Authentication

Many modern enterprises have outsourced portions of their authentication development, maintenance and troubleshooting. If done well it can save the enterprise money. If done poorly, it can create security holes or, cause enterprise failures.

Usernames and Password for Identification and Authentication

A common way to authenticate users is to assign each authorized user of a specific system a unique username/password combination. The username identifies the user and the password authenticates him; in other words, a human user proves his/her identity is true to the nonhuman system. A password is "a word, a phrase, or combination of miscellaneous characters that authenticates the identity of the user". However, the only matter that is sure is that the username and password combination agrees with a username/password combination in the system's database of valid and authorized users. If the user logs into the system remotely, the only element that the system is sure of is the combination entered matches a stored combination for a user of the system.

Rubens emphasized that the Gartner research house reported 94% of businesses only require a username/password combination to log into their respective computer systems. That popularity and reliance illustrates a lot of commercial trust in the simple philosophy of identification and authentication of access. Passwords are a simpler and cheaper security measure compared to other security hardware and software. Passwords can protect users' personal information such as private documents, financial data, identity data, or social security numbers. Passwords can also protect professional data, which could mean intellectual property, trade secrets, financial data, human resource records, or customer information. The access or loss

of any of this data in the hands of the wrong party could be detrimental and disabling to the person, the profession, or the proprietor.

As Schneier cautioned, "The problem with passwords is that they're too easy to lose control of. People give them to other people. People write them down, and other people read them. People send them in email, and that email is intercepted. People use them to log into remote servers, and their communications are on. They're easy to guess. And once that happens, the password no longer works as an authentication token because you can't be sure of who is typing that password in".

The commonality in all of these passwords flukes is "people"—humans with that imperfect human nature that corporations trust their most valuable asset to in the security framework.

The popularity of username/password combinations reveals the reliance corporations and institutions have on people keeping their passwords private. Considering the unpredictable and imperfect human nature of people, the key to security with username/password combinations is educating and training the users to exercise a regimen that safeguards and secures accurate identification and authentication of the user.

Password authentication

In **password-authenticated key agreement** method is an interactive method for two or more parties to establish cryptographic keys based on one or more party's knowledge of a password.
An important property is that an eavesdropper or man in the middle cannot obtain enough information to be able to brute force guess a password without further interactions with the parties for each (few) guesses. This means that strong security can be obtained using weak passwords.

Types

Password-authenticated key agreement generally encompasses methods such as:

- Balanced password-authenticated key exchange
- Augmented password-authenticated key exchange
- Password-authenticated key retrieval
- Multi-server methods
- Multi-party methods

In the most stringent password-only security models, there is no requirement for the user of the method to remember any secret or public data other than the password.

Password authenticated key exchange (PAKE) is where two or more parties, based only on their knowledge of a password, establish a cryptographic key using an exchange of messages, such that an unauthorized party (one who controls the communication channel but does not possess the password) cannot participate in the method and is constrained as much as possible from brute force guessing the password. (The optimal case yields exactly one guess per run exchange.) Two forms of PAKE are Balanced and Augmented methods.

Balanced PAKE allows parties that use the same password to negotiate and authenticate a shared key. Examples of these are:

- Encrypted Key Exchange (EKE)
- PAK and PPK
- SPEKE (Simple password exponential key exchange)
- Dragonfly-- IEEE Std 802.11-2012, RFC 5931, RFC 6617
- J-PAKE (Password Authenticated Key Exchange by Juggling) -- A variant that is probably not encumbered by patents.

Augmented PAKE is a variation applicable to client/server scenarios, in which the server does not store password-equivalent data. This means that an attacker that stole the server data still

cannot masquerade as the client unless they first perform a brute force search for the password. Examples include:

- AMP
- Augmented-EKE
- B-SPEKE
- PAK-Z
- SRP (Secure Remote Password protocol) -- designed to be not encumbered by patents.

Password-authenticated key retrieval is a process in which a client obtains a static key in a password-based negotiation with a server that knows data associated with the password, such as the Ford and Kaliski methods. In the most stringent setting, one party uses only a password in conjunction with N (two or more) servers to retrieve a static key. This is completed in a way that protects the password (and key) even if N-1 of the servers are completely compromised.

Protecting Password

A Strong Password that is memorized, never reused, and never shared with anyone, is a very secure password.

The problem is, the more accounts we have, the more passwords we have. On top of that, the more complex we are forced to make those passwords, the harder it is to simply memorize all of them.

Sometimes when we near a breaking point for mentally managing our passwords, we start cutting corners. We make our passwords simpler. We use the same password for multiple accounts. Or even worse, we start writing down our passwords in little notebooks. Or we attach Post-It-Notes to our computer, displaying our passwords for anyone that walks past.

If you are in the habit of cutting corners in any of the ways listed (or any other way that could easily reveal your password), it's time to break those habits right now. Destroy those post-it-notes, never use "password" as a password again, and make sure your password for the celebrity gossip web site isn't the same as your credit card password.

Password Managers helps the people to remember their passwords. Password managers allow you to securely store all of your passwords in one encrypted location that no one can access without logging in. All you have to do is remember your master password to unlock your password manager and get to your passwords.

Characteristics of *weak* passwords

- Based on common dictionary words
- Including dictionary words that have been altered:
- Reversed (e.g., “terces”)
- Mixed case (e.g., SeCreT)
- Character/Symbol replacement (e.g., “$ecret”)
- Words with vowels removed (e.g., “scrt”)
- Based on common names
- Based on user/account identifier
- Short (under 6 characters)
- Based on keyboard patterns (e.g., “qwerty”)
- Composed of single symbol type (e.g., all characters)
- Resemble license plate values are difficult for you to remember

Examples of weak passwords

- Recycling passwords
- Recording (writing down) passwords
- To use of previously recorded passwords (combination of above practices)
- To use of password on two or more systems/contexts

- Especially risky when passwords are reused in low-trust systems (e.g., online gaming) since increased exposure

Characteristics of strong passwords

- It contain at least *one of each* of the following:
  - digit (0..9)
  - letter (a..Z)
  - punctuation symbol (e.g., !)
  - control character (e.g., ^s, Ctrl-s)
- It based on a verse (e.g., passphrase) from an obscure work where the password is formed from the characters in the verse
  - e.g., "ypyiyp" derived from the title of this module
  - sometimes referred to as a *virtual password* are easily remembered by you but very difficult (preferably impossible) for others to guess

Examples of Strong Passwords

- never recycle passwords
- never record a password anywhere
- exceptions include use of encrypted password "vaults"
- To use a different password for each system/context
- be aware Trojan horse programs can masquerade as login prompts so always reset the system as appropriate to obtain a trusted login prompt
- check for keyboard buffer devices/software that intercept keystrokes (including password capture)
- change password occasionally
- change your password immediately if you suspect it has been "stolen"
- "passwords should be protected in a manner that is consistent with the damage that could be caused by their compromise."
- monitor for possible eavesdroppers during entry of password
- do not use the "Remember Password" feature of applications (e.g., Microsoft Internet Explorer.
- inquire about proactive password checking measures with your system administration .

Protected Password

A strong password is one that's hard to crack. A strong password must have all of the following:

- Your password must be no fewer than eight (8) characters in length. **However, a good choice is a "pass phrase" composed of four (4) words and punctuation.** A pass phrase is a longer version of a password and is therefore more secure. A pass phrase is typically composed of multiple words.
  - Note: Though technology constraints may impose maximum length or other restrictions, use of pass phrases shall be supported where possible and practical.
  - Examples of pass phrases:
    - I like ice cream.
    - Turn Off Cell Phones!
    - It was hot today.
    - Cal Poly Broncos rule!
- At least three of the following four types of characters:
  - It must have at least one number.
  - It must have at least one uppercase letter.
  - It must have at least one lowercase letter.
  - It must have at least one symbol (!,@,#,$,^).

Examples of Extremely Bad Passwords

- Your name in any form - first, middle, last, maiden, spelled backwards, nickname or initials
- Your user ID or your user ID spelled backwards
- Part of your user ID or name
- Any common name, such as Joe
- The name of a close relative, friend or pet
- Your phone number, office number or address
- Your birthday or anniversary date
- Simple variants of names or words (even foreign words), simple patterns, famous equations or well-known values
- Your favorite sports team (NFL, NBA, MLB, etc.)
- Your license plate number, your social security number or any all-numeral password
- Names from popular culture (e.g.: Beatles, Spiderman, etc.)

Creating a Stronger Password

You should follow these guidelines when creating a password:

- Do not use your user name or any part of your real name.
- Do not use a single word in a common language. There are tools for hackers that search through electronic dictionaries, trying every word.
- Avoid characters other than those above, such as accented characters (áèôü) or characters from other alphabets (Ρωσικά, Греческий). The basic system will handle these passwords, but you may not be able to enter them correctly on web pages.
- Spell a word backwards (anomopyloplac1#).
- Insert a number (calpo7lyPomona) or punctuation (go!Broncos).
- Use weird capitalization (remember that it counts), or combine words (broNCOsrOOL!)).
- Use the first letters of each word in a phrase ("I can never remember my stupid password!" = Icnrmsp!).
- Combine things you will remember ("I like to eat broccoli and listen to Beethoven = broCColi@bEEthoven).
- Consider using a pass phrase instead of a password.

Password Managers

A password manager is software for storing all your passwords in one location that is protected and accessible with one easy-to-remember master passphrase. It is one of the best ways to keep track of each unique password or passphrase that you have created for your various online accounts—without writing them down on a piece of paper and risking that others will see them. When using a password manager, you have one master passphrase that protects all of your other passwords. This leaves you with the ease of having to remember only one.

Types of Password Managers

As Neil Randall pointed out in PC Magazine over a decade ago, "Password management utilities have proliferated with the growth of the Internet and, as Web users log on to more and more password-protected sites, have become almost indispensable tools." There are many types of password managers. A desktop password manager is software you install on your computer's hard drive; it stores your user name and password only on that computer. You can use a portable password manager on your smart phone and other portable devices. Or you may choose to store your passwords on the website of a password management provider or choose multi-factor authentication, where you use a combination of ways to access a password manager on your desktop; for example, a smartcard or USB drive plus a password or, perhaps, a fingerprint. Some password managers can create new passwords for you. This eliminates the need for you to come up with dozens of unique and complex passwords and passphrases. In PC World, Paul Mitchell describes a new type of password manager that eliminates the worry about where your password manager is located: "The makers of an emerging breed of password managers are striving to

provide secure online access to your passwords in the cloud and give you a synchronized, local copy of your password database on every computer and mobile device, no matter what operating systems, browsers or mobile platforms you use." If all the information is stored in the cloud, you can access it from any of your devices at any time. Moreover, in effect, the cloud provider creates a backup of your password manager file. If you do not regularly back up your desktop files, a cloud-based password manager may have important features for you to consider.

Choosing a Password Manager

Consider the type of password manager that best suits how and where you work. This is where research into the type of password manager is necessary. Ask yourself what type of passwords you will be storing and where you will most often access these sites. For example, if you have passwords only for sites that you access at home, you would not need the password manager to be stored on your mobile device. If you store a password manager on one computer and need to access your passwords on another computer, you run into problems. On the other hand, if you are using only one computer, the storage decision becomes easier. If you use a generator of one-time passwords for all your accounts, you do not have a set of passwords to store—though you may have a set of usernames.1 You need to consider whether acquiring a password manager is the best way to handle your usernames. If you have a mix of passwords you choose and one-time passwords that are generated for you, a password manager can be useful for the passwords you choose.

After you know your needs, you can investigate particular products. When researching the products, determine the security measures of each. Does the password manager use strong encryption? Does it have a lockout feature? Does it include protection from malicious activity, such as keystroke logging—and which kinds of activity? Evaluate ease of use and convenience. Look at the functionality and the interface features and think about how you will like them over the long term. Also examine support from the vendor/provider.

Look for (and evaluate) online documentation, and find out how the company interacts with its customers: email? telephone? chat? other ways? Consider cost. Is there a one-time cost or a recurring fee? Some password manager vendors provide a free trial period or charge for certain features. If the latter, which features do you consider worth the cost? Supplement your own evaluation by searching the web for articles on the top-rated password manager and analyses of the strengths and weaknesses of various products Finally keep risks in mind.

Note particularly that there is both convenience and risk associated with storing your passwords in the cloud, as noted in a previous US-CERT paper2 and there is the potential for attacks on cloud password managers. In May 2011, Brennan Slattery, reported in a PC World that the provider of an online password manager identified unusual network traffic of a size that could indicate an email address and password compromise.

All customers were asked to change their master password. Remember also that there is a risk with using your password manager in public locations, specifically if you leave the password manager open in the background on the computer. Also if you open your password manager on a public computer you may be taking the risk of key logging software being installed on the computer. This software can capture the information that you type on the keyboard, and a malicious user could steal your master password. In all cases, you must protect your master password well; it's best to memorize it rather than write it down.

LEVEL II

In today's environment, technology has made to access the information worldwide quicker and easier. Telecommunication made everyone to capture, store and transmit the information to every nook and corner of the world. The rapid development of information technology provides new possibilities for automating tasks and enriching the lives of the people.

Technology refers to methods, tools, procedures to handle applied input and output relations to perform a specific task. Technology which is adopted to store, process and transmit the information from one place to another place is called Information Technology. Computer and other electronic devices like ATM, mobile phones are used to store data, process data and transmit the data to the place we need.

Cyber means the use of Internet technologies and computers. It includes computers, networks, software, data storage devices, Internet, websites, emails, ATM machines etc. **Cyber security** is **security** applied to computers, **computer** networks, and the data stored and transmitted over them. The field is of growing importance due to the increasing reliance of **computer** systems in most societies.

Cyber space

Cyberspace is "the notional environment in which communication over computer networks occurs." It is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology (ICT), devices and networks.

Unlike most computer terms, "cyberspace" does not have a standard, objective definition. Instead, it is used to describe the virtual world of computers. For example, an object in cyberspace refers to a block of data floating around a computer system or network. With the advent of the Internet, cyberspace now extends to the global network of computers. So, after sending an e-mail to your friend, you could say you sent the message to her through cyberspace.

Cyber space is a domain characterized by the use of electronic and electromagnetic spectrum to store, modify and exchange data via network systems and associated physical infrastructure. The Cyber space is borderless and actions in the cyber space can be anonymous. These features are being exploited by adversaries for perpetration of crime in the cyber space. The scale and sophistication of the crimes committed in the cyber space is continually increasing thereby affecting the citizens, business and Government. As the quantity and value of electronic information have increased, the criminals and other adversaries embraced the cyber pace as a more convenient and profitable way of carrying out their activities anonymously. Every action and reaction in cyberspace has some cyber legal perspectives. Cyber space includes Computer, Mobile phone, ATM, Data storage device, Software, Network, Website, E-mail

Cyber law

Cyber law is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less a distinct field of law in the way that property or contract are as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. Cyber law is an attempt to integrate the challenges presented by human activity on the Internet with legacy system of laws applicable to the physical world.

Cyber law is the law which regulates the operations performed by the user via network by electronic means. Cyber law is important because it touches almost all aspects of transactions and activities involving the internet, World Wide. In other words, we can say cyber law regulates

the cyber space. To protect the cyber crime over Internet, this law is passed to protect the Internet cyber crime. This law is approved by the government.

Cyber law includes and encompasses laws relating to

- Cyber crimes
- Electronic and digital signatures
- Intellectual property
- Data protection and privacy

Features of cyber law:

- Cyber law contains a set of rules and guidelines
- Cyber law provides for legal internet activities
- Cyber law specifies the illegal activities which are punishable under law
- Cyber law provides legal framework for all the activities which are carried out through the network.

Significance of cyber law:

Information technology has varied applicability in almost all aspects of our life. Some of the areas are science and engineering, business, education and entertainment. Mostly we are relying upon information technology to carry out our day to day activities. Companies are able to carry out electronic commerce using the legal infrastructure provided by the Act. Act allows Government to issue notification on the web thus heralding e-governance. Cyber law Protect Computer fraud and unauthorized access. Consumers are now increasingly using credit cards for shopping. Most people are using email, cell phones and SMS messages for communication as well as Deal with Internet Banking Transactions.

Criminal activities of cyber law

Though we are utilizing information technology frequently in some of the areas, we have to be equally caution. For example, due to the anonymous nature of the internet, it is possible for the fraudulent people to involve in several of criminal activities. Some of the criminal activities are

1. Launching of malicious software in the form of worms, viruses, Trojans, spyware, adware, etc,
2. Computer hacking which is a thread to the secrecy of the information, document and data.
3. Downloading unauthorized software.
4. Selling illegal articles such as narcotics, weapons, etc.,
5. Gambling activities through online.
6. Stealing of money from banks using networks.
7. Credit card frauds.
8. Cyber stalking, cyber defamation, indecent & abusive mails, unauthorized and incorrect information and news.
9. Stating false advertisements in the web page, e-mail and SMS.

To overcome the above said criminal activities, various security measures are applied. Still, lots of cyber crimes are going on. In order to protect people from cyber crimes, there is a need for cyber law.

Advantages of cyber law

Cyber law has the following advantages:

1. Cyber law regulates the transaction which is carried out through cyber space.
2. It provides legal infrastructure for e-Commerce transactions.
3. It authorized the certifying authorities for issuing digital signature certificates.

4. It validates the digital signature.
5. E-mail is considered as a valid message and legally acceptable in a court of law.
6. It is possible for the users to use against the fraudulent people who commit cyber crimes and cause losses.
7. Statutory remedy is available for any losses which occur due to cyber crimes.

Cyber law-Governance

Cyber law governs the four major parts. They are

1. Cyber crimes
2. Electronic signature
3. Intellectual property and
4. Data privacy

1. Cyber crimes

Cyber crimes are illegal activities done with the use of network linked technology. Fraudulent people target the computers to attack the confidentiality and the information of the victims. They use computers as a tool for cheating, gambling, illegal copying etc. Some of the people commit a crime by downloading unauthorized software, contraband, stealing the trade secrets, accessing the website in an unauthorized way. So it is more important to govern the activities which are involved in cyber space.

2. Electronic signature

With the advancement in technology, the use of the internet for business transactions has also increased. Most of the transactions require you to provide important information about yourself. This information is processed to complete the transactions. However, the business organizations need to verify that the information that you provide is correct and authentic. To ensure this, a digital signature is used by users. A digital signature is similar to a handwritten signature.

Functions of digital signature:

4. To authenticate the identity of the user of the signature.
5. To ensure that the contents of the signed documents cannot be changed or distorted.
6. To ensure non-repudiation that means the user of the signature cannot deny sending the information that was digitally signed.

   Digital signature provides improved security, which increases the confidence of the user of digital information exchange.

Handwritten signature cannot be stolen but can be easily forged. However, digital signature is impossible to forge. The only problem with the digital signature is that they can be stolen if care is not taken. Therefore, digital signature should be kept confidentially.

To make the electronic document genuine and legally acceptable, digital signature is necessary. It authenticates the person who signs and the message as genuine and honest. Unlike handwritten signature, you can see multiple digital signatures in different ways for various purposes. You can see the same signature whenever you have to authenticate a document. However, you can have a number of digital signatures depending upon the requirement and purpose.

Digital signatures are created using public key cryptography. When a user implements a digital signature, two keys are generated. One of these keys is a private key that is kept secret. The other is a public key, which is available to all. The private key is used to generate a digital signature that is used to sign an electronic document.

Consider that you want to digitally sign an electronic document. First, a special function in the encryption software automatically produces a unique summary of the document that has to be encrypted. This summary is called a message digest. Then, the message digest is encrypted with your private key to produce the digital signature.

After the signature is created, you send the original document and signature to the recipient who uses your public key to verify the signature. The public key does not verify the signature even if there is a minor alteration to the file. This is because the alteration results in a different message digest. This ensures that the message that you send is not modified by anyone. The signature is also not be verified if the private and public keys do not modified by anyone. The signature is also not be verified if the private and public keys do not match.

A digital signature ensures that the receiver does not accept an altered message. Digital signature also ensures non-repudiation. Non-repudiation is achieved through cryptography methods. If an individual uses a digital signature, the signature prevents the individual from denying having performed a particular action related to the digitally signed data. Digital signature provides evidence to a third party that an action has occurred. Digital signatures can be specifically used to provide evidence in the non-repudiation of approval, submission and receipt during online transaction.

If person conducts transaction by using digital signature, it implies that the person has used the private key. This private key is assumed to be in safe custody of the holder and is inaccessible to the others. In addition it is not possible to forge the digital signature. Therefore only the sender of the message could have generated the message that results in a transaction.

3. Data privacy

Data privacy is very much required for individual business establishments' educational institutions and government. Normally password and encryption technology are used as a security measure to protect data in cyber space. In spite of this, password is stolen and data is extracted. The password is stolen by way of matching the dictionary words with the password. So everyone must be cautious while framing the password for data privacy. With encryption, the data can be securely transmitted via internet. Encryption can protect the data at the simplest level by preventing other people from accessing it.

4. Intellectual property

Intellectual property refers to intangible or non-physical goods. It is protected by copyright for written works, patents for inventions and trade marks for brands, names and logo. Intellectual property relating to computer and other electronic means are legally covered under cyber law.

Facilitating function of cyber law

Today adversaries are developing, selling and distributing malicious code with ease, maximizing their gains and exploiting the fact that attribution is a challenge. E-business, e-banking, e-shopping, e-receipts & payments, e-transmission of the documents, e-education, e-medicine, e-information, e-database, e-entertainment, e-engineering are the major functions of cyber law.

Major issues in cyber space

Malware is getting stealthier, more targeted, multi-faceted and extremely difficult to analyze and defeat even by the experts in the security field. Organized crime is fast growing and targeting the exponential growth of on line identities and financial transactions. There is increasing evidence of espionage, targeted attacks and lack of traceability in the cyber world as state and non-state actors are compromising, stealing, changing or destroying information and therefore potentially causing risk to national security, economic growth, public safety and competitiveness.

Major issues related to cyber space:

1.Developments of cyber space pave the way for cyber crimes.

2.In some cases, identification of the user is not possible.

3.E-mail address has digital identity, but it does not show the reliable identity.

4. Passwords are used as identity but are shared easily.
5. Internet protocol (IP) addresses serve as an address for a computer. But it does not identify the user of a computer.

The Need for an Indian Cyber Law

In today's techno savvy environment, the world is becoming more and more digitally sophisticated and so are the crimes. Internet was initially developed as a Research and information sharing tool and was in an unregulated manner. As the time passed by it became more transactional with e-business, e-commerce, E-governance and e-procurement etc. Today adversaries are producing, selling and distributing malicious code with ease, maximizing their gains and exploiting the fact that attribution is a challenge. Malware is getting stealthier, more targeted, multi-faceted and extremely difficult to analyze and defeat even by the experts in the security field. Organized crime is fast growing and targeting the exponential growth of on line identities and financial transactions. There is increasing evidence of espionage, targeted attacks and lack of traceability in the cyber world as state and non-state actors are compromising, stealing, changing or destroying information and therefore potentially causing risk to national security, economic growth, public safety and competitiveness. All legal issues related to internet crime are dealt with through cyber laws. In today's highly digitalized world, almost everyone is affected by cyber law. As the number of internet users is on the rise, the need for cyber laws and their application has also gathered great Momentum. For example

- Almost all companies extensively depend upon their computer networks and keep their valuable data in electronic form.
- Government forms including income tax returns, company law forms etc are now filled in electronic format.
- Consumers are increasingly using credit cards for shopping.
- Most people are using email, cell phones and SMS messages for communication.
- Even in "non-cyber crime" cases, important evidence is found in computers / cell phones e.g. in cases of divorce, murder, kidnapping, tax evasion, organized crime, terrorist operations, counterfeit currency etc.
- Cyber crime cases such as online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, pornography etc are becoming common.
- Digital signatures and e-contracts are fast replacing conventional methods of transacting business.
- Almost all transactions in shares are in demat form.

Technology is never a disputed issue but for whom and at what cost has been the issue in the ambit of governance. The cyber revolution holds the promise of quickly reaching the masses as opposed to the earlier technologies, which had a trickledown effect. Such a promise and potential can only be realized with an appropriate legal regime based on a given socio-economic metrics

Plans of the National Information Technology Policy (NITP)

The National Information Technology Policy (NITP) says that there is an urgent need, not only to computerize government departments and ministries but a central mechanism is required, so that government can get feedback from citizens electronically. This would also require putting up information kiosks; government websites; complete intranet connectivity amongst government departments and information flow from government to citizens and vice versa.

Issue of smartcards wish is more useful and intelligent version of today's credit card, containing micro chips encoded with various class of confidential information such as -

- Personal financial information, allowing transfers from one's bank to various payee and
- Personal medical information' accessible only to qualified medical care givers

Unless backed by efficient legislations, the ambitions of the NITP, it is afraid, may remain unaccomplished. However, the NITP has acknowledged the urgency for a cyber law for our country. The NITP has underscored the need for an Indian cyber law thus:-

The outdated Indian laws required a quick change. It's high time that we change vintage telegraph Act of 1885, so that the Indian people and telecom companies can freely breathe. It is also essential to introduce laws against computer crime and such other cyber laws that would help build the National Information Infrastructure. The laes have to take into consideration, the emerging use of Electronic Data Interchange (EDI), Electronic Commerce, Electronic Fund Transfer, Electronic Cash, Copyright and Digital Intellectual Property Rights. For example, one may require to change the Evidence Act to recognize Digital signature. Changes in Evidence Act, 1872 Indian Penal Code 1860 and Indian Patents Act General Clauses/Act would be undertaken to recognize emerging technologies, keeping in view of the following:

- Preventing of computer crimes
- Digital Signatures especially as related to Electronic Fund Transfer
- Copyright and Digital Intellectual Property Rights especially with regards to Internet and World Wide Web
- Electronic Governance
- Computerization of Land Records
- Bar Coding of all consumer goods and related amendments in the Weight and Measures Act
- Cryptography and Encryption
- Privacy of data

The Need for protection of Data

Data Protection has been defined to include-

- The legal safeguards of people's rights to see what information may be held about them in a computer database, and

- The protection from theft, destruction, or damages of software (programs) and data held in a computer's memory. The second type of data protection is also often called data security.

Examples of the former are Government departments and commercial companies that hold personal data in computers. For example, a company may have a computer database listing the names and addresses of the customers. At ax office may have a similar computerized list of everyone who pays income tax. Some countries have laws giving various rights to people listed in such database. In the UK, the 'Data Protection Act 1984' safeguards the individual's right to see his or her database entries, alter inaccuracies, or in some cases have it deleted. According to this Act, organization holding computerized personal data must register with the 'Data Protection Registrar'. Organizations registered with the Data Protection Registrar must show any individual whatever information they hold on that person, except in a few instances. Any organization that ought to have registered, but has not registered, is committing a criminal offence. Similarly laws operate in other countries also, especially in Europe.

As far as the latter category is concerned, a technologically advanced India remains handicapped for want of legal support in implementing many of the technological innovations. The absence of law relating to digital signature and encryption prevents our company from implementing Electronic Fund Transfer (EFT) in a big way, apart from depriving the country of the benefits of E-Commerce. Apart from the above, the absence of law and legal deterrents relating to computer crime emboldens many a computer criminal in the country to indulge in computer crime. The absence of the provisions enabling electronic data as 'admissible evidence' in the courts has put our country decades back to other nations.

Transactions in securities

With the e-commerce service you can now make transactions over the Internet with added security. With the growing emphasis on security for online transactions, people are looking for the safest and most secure online payment channel. We recognize this need and have enabled an additional security mechanism called Verified by Visa (VbyV) to prevent fraud in e-commerce transactions over the Internet. You need to enter the VbV password in addition to your CVV and card no. to confirm your credibility when you make online transaction payments. It is to ensure your transactions and as secure as possible and your card is not being misused.

Transactions take place in dematerialized securities in a stock exchange, either directly or through the Internet, is a commercial activity taking place through the cyber medium. Therefore Cyber Law has become pertinent for the legal validation of transactions in electronic securities. The Cyber law has been drafted by the department of Electronics, Government of India.

Securities transactions are worth millions of rupees and any misadventure in the cyber medium can cause damages to the capital market in particular and to the economy in general. In this context, the of extent applicability of Cyber Law in transactions involving Soft Securities has to be analyzed, and loopholes plugged. An in-depth study of the systematic risks involved in securities transactions in the cyber medium should be researched and suitable remedies suggested.

Electronic Banking

Cyber Law has a very vital role to play at the application level, because of the critical nature of financial data transfer. The financial messages should have the under noted features:

- The receipt of the message at the intended destination (data transmission)
- The content of the message should be the same as the transmitted one (data integrity)
- Sender of the information should be able to verify its receipt by the recipient (data acknowledgement)
- Recipient of the message could verify that the sender is indeed the person (data authenticity)
-Information in transit should not be observed, altered or extracted (data security)
- Any attempt to tamper with the data in transit will need to be revealed (data security)
- Non-repudiation (non repudiation of the data)

These features take down essentially to

- Authentication
- Authorization
- Confidentiality
- Integrity
-Non-repudiation

Authentication:

To verify the identity of the sender of the message to the intended recipient to prevent spoofing or impersonation

Authorization:

Authorization means to control the access to specific resources for unauthorized persons

Confidentiality:

To maintain the secrecy of the content of transmission between the authorized parties. Confidentiality is the concealment of information or resources'. The need for keeping the information secret arises from the use of computers in sensitive fields such as government and industry. For example, military and civilian institutions in the government often restrict access to information those who need that information. The first formal work in the computer security was motivation of the military's attempt to implement controls to enforce a "need to know"

principle. This principle also applies to industrial firms, which keep their proprietary designs secure their competitors try to steal the designs. As a further example, all types of institutions keep personnel records secret.

Access control mechanisms support confidentiality. One access control mechanism for preserving confidentiality is cryptography, which scrambles data to make it incomprehensible. A cryptography key controls access to the unscrambled data, but then the cryptographic key itself becomes another datum to be protected.

Example: Enciphering an income tax return will prevent anyone from reading it. If the owner needs to see the return, it must be deciphered. Only the possessor of the cryptographic key can enter it into a deciphering program. However, if someone else can read the key when it is entered into the program, the confidentiality of the tax return has been compromised.

Example: The user of Computer A sends a message to the user of the computer B. Another user C get access to this message, which is not desired, and therefore, defeat the purpose of confidentiality. For an example an email message is send by A to B, which is accessed by C with the permission of both.

Other system-dependent mechanisms can prevent processes from illicitly accessing information. Unlike enciphered data, however, data protected only by these controls can be read when the controls fail or bypassed. Then their advantage is off-set by a corresponding disadvantage. They can protect the secrecy of data more completely than cryptography, but if they fail or evade, the data becomes visible.

Confidentiality also applies to the existence of data, which is sometimes more revealing than the data itself. Access control mechanisms sometimes conceal the mere existence of data; less the existence itself reveal information that should be protected.

Resource hiding is another important aspect of confidentiality. Sites often wish to conceal their configuration as what systems that are using; organization may not wish others to know about specific equipment because it could be used without authorization or in inappropriate ways, and a company renting time from a service provider may not want others to know what resources it is using. Access control mechanisms provide these capabilities as well.

All the mechanisms that enforce confidentiality require supporting services from the system. The assumption is that security services can rely on the kernel, and other agents, to supply correct data. Thus, assumptions and trust underlie confidentiality mechanisms.

Integrity:

To ensure that no changes or errors are introduced in the messages during transmission. Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized changes. Integrity includes data integrity (the content of the information) and origin integrity (the source of the data, often called authentication). The source of the information may bear on its accuracy and creditability and on the trust that people place in the information. This illustrates the principle that the aspect of integrity known as creditability is central to the proper functioning of the system.

Integrity mechanisms fall into two classes: prevention mechanisms and detection mechanisms. Prevention mechanisms seek to maintain the integrity of the data by blocking any unauthorized attempts to change the data or any attempt to change the data in unauthorized ways. The distinction between these two types is important. The former occur when a user tries to change the data which has no authority to change. The latter occurs when a user authorized to make certain changes in the data tries to change the data in the other ways.

Adequate authentication and access controls will generally stop the break-in from the outside, but preventing the second type of attempt requires very different control. Detection mechanisms do not try to prevent violations of integrity; they simply report that the data's integrity is no longer trustworthy. Detection mechanisms may analyze system events to detect problems or may analyze the data itself to see if required or expected constraints still hold. The mechanisms may

report the actual cause of the integrity violations (a specific part of a file was altered), or they may simply report that the file is now corrupt.

Working with integrity is very different from working with confidentiality. With confidentiality, the data is either compromised or it is not, but integrity includes both the correctness and the trustworthiness of the data. The origin of the data, how well the data is protected before it arrived at the current machine, and how well the data is protected on the current machine all affect the integrity of the data. Thus, evaluating integrity is often very difficult, because it relies on assumptions about the source of the data and about trust in that source-two underpinning of security that are often overlooked.

Non-repudiation:

To ensure that an entity cannot later deny the origin and receipt and contents of the communication

There should be an appropriate institutional arrangement for key management and authentication. This is normally done through Certification Agencies. For the banking and financial sectors' the RBI should appoint a suitable agency/institution as the Certificate Agency. There should also be an institutional arrangement for appropriate assessment of participants of the financial network in terms of their credit-worthiness, financial soundness, etc. These assessments will provide valuable input to the banking and financial sector.

Initially the Indian Financial Network (INFINET) will be a Closed Used Group (CUG) network, but in due course this network will have to be connected to public networks like the Society for World-wide Interbank Financial Telecommunication (SWIFT) etc. It is essential to look at the possibility of having firewall implementations and they need to meet the following criteria:

- All in and out traffic must pass through the firewall. The firewall should check and authorize the traffic. The firewall in itself should be immune to penetration.
- Implementation of firewalls can be done using packet filtering routers, application and circuit level gateways and also network translation devices.
- State full multilayer inspection gateways combine the advantages of the above and also give a better performance, flexibility and security. This environment can handle all kinds of applications, namely, Transmission - Control Protocol (TCP), User Datagram Protocol (UDP), Remote Procedure Call (RCP), Internet Control Message Protocol (ICPMP) etc. New applications can be added easily and this environment is totally transparent to end-users.
-Firewalls are used to implement access control security as well as to provide for user authentication and to ensure data integrity by using encryption. It is important that the banks have their own security policy and then design security solutions accordingly. Regular reviews of security Policies and their implementation are also important.

Highly secured (e.g., funds related), secured, non-secured messages should be clearly demarcated in the security policy. Banks are, therefore, advised to have dedicated groups with enough competence and capability.

Since security is the prime concern for the banking and financial sector, continuous research should be carried out as is done in the internet community. Institution like IDRBT should have collaborative arrangements with national and international agencies for carrying out research in this field. Such Institutions could develop Tiger teams (hackers) and the banks can engage the team to test and determine the strength of the firewall implementation.

Mobile information security

Modern day smart phones offer wireless internet connectivity Cyber security has been an important topic in the today's scenario. In fact, a recent study by the Center for Strategic and International Studies wrote, "Cyber security is among the most serious economic and national security challenges we face in the twenty-first century". For a company to achieve effective

mobile commerce security and ultimately consumer trust the security mechanisms will constitute as a security risk. The mechanisms are:

Authorization – It means ensuring authorized uses of systems and performance of business functions by authorized users only.

Authentication – Authentication is establishing that parties to an electronic transaction or communication are who they claim they are.

Integrity- Ensuring that data on the host system or in transmission are not created, intercepted, modified or deleted illicitly.

Confidentiality- Warranting that data are only revealed to parties who have a legitimate need to know it or have access to it.

Availability - Ensuring that legitimate access to information and services is provided. It should be available every time when it is required.

Non-repudiation - If a party to some transaction or communication later denies that it has ever happened, some mechanism is in place to facilitate dispute resolution.

Privacy - Ensuring that customers' personal data collected from their electronic transactions are protected from indecent and/or unauthorized disclosure.

Hackers

Hacking in computers is the unauthorized access and use of networked computer systems. Hackers can be outsiders or company members. They can use the Internet to steal or damage the data.

Some hackers who commits only electronic breaking and entering; they can access the system and reads some files but neither steals nor damages anything. Hackers can monitor mails, file transfers to extract passwords and also steal network files. A hacker may also use remote services that allow one computer on network to execute programs on another computer to gain privileged access within a network.

Telnet an Internet tool for interactive use of remote computers, can help hackers discover information and to plan other attacks. Hackers have used Telnet to access a computer mail port, to monitor the messages, passwords and other information about user accounts and network resources. These are the crimes hackers commit on the network.

Hacking Process

Common Hacking Tactics

Denial of Service

This is a common networking prank. By hammering a website's equipment with too many requests for information, an attacker can effectively clog the system, slowing the performance or even crashing the system. This method of overloading the computers is sometimes used to cover up an attack.

Hackers use Denial of Service (DoS) attacks to prevent legitimate uses of computer network resources. DoS attacks are characterized as

- Attempts to flood a network.
- Attempts to disrupt connections between two computers.
- Attempts to prevent an individual from accessing a service.
- Attempts to disrupt service to a specific system or person.

Those on the receiving end of a DoS attack may lose valuable resources, such as their e-mail services, Internet access or their Web server. Some DoS attacks may eat up all your bandwidth or even use up all of a system resource, such as server memory.

Sniffer

Sniffer is the programs that secretly search individual packets of data as they pass through the internet, capturing the passwords and contents. It is also called as spoofer. It is a standalone program to intercept and analyze certain data. For example a sniffer can intercept and analyze network traffic and catch certain data, for example passwords. Trojans sometimes use sniffing capabilities to steal passwords and user information from infected computers. There also exist a lot of commercial and free sniffers. They can be used to analyze network traffic for performance, security issues and faults.

Sniffer is a Network analyzing tool. Network analyzing tools are used to monitor the traffic conversations that occur across the network. Often the information obtained from a sniffer can be used to figure out exactly how devices are communicating. But the use of a sniffer is not limited to troubleshooting, it can also be used to help train, design and operate devices on a network.

Spoofing

Spoofing is the process of faking the websites or mails to trick users into passing along critical information like credit card numbers or passwords.

A spoofing attack is user on a network; in order to launch attacks against network hosts, steal data, spread malware etc. Many of the protocols do not provide mechanisms for authenticating the source or destination of a message. They are thus vulnerable to spoofing attacks when extra precautions are not taken by applications to verify the identity of the sending or receiving host. Spoofing attacks which take advantage of protocols may be mitigated with the use of firewalls capable of deep packet inspection or by taking measures to verify the identity of the sender or recipient of a message.

Trojan horse

Trojan horse is a malicious, security breaking program that is disguised as something benign, such as directory lister, archiver, and game. Trojan is a type of virus that normally requires user to perform some action before the payload can be achieved. It is a program that, unknown to the user, contains instructions that exploit a known vulnerability in some software.

Worm

A worm is a malicious program that propagates itself over a network, reproducing itself as it goes. Worm allows hackers to hack your complete network from the location. This infection allows hackers to steal data like credit card numbers, passwords and other personal information. Worm is critical; it may crash the Operating system.

Malicious Applets

A malicious applet is any applet that attacks the local system of a Web surfer. Malicious applets are written by researchers, crackers, and Net miscreants to annoy and damage Java users. They can even seriously damage a Java user's machine. These are tiny programs, written in the popular java computer language, that misuse your computer resources, modify files on the hard disk, send fake mails or steal passwords. Any applet that performs an action against the will of the user who invoked it should be considered malicious.

Logic bomb

A logic bomb is a piece of programming code buried within another programme, designed to perform some malicious act. It is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting important files of a company or organization, which will lead problems to the organization.

Software that is inherently malicious, such as logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates, such as Wednesday the 12th or Independence Day. Viruses that activate on certain dates are often called "Time bombs".

Threat

A threat is anything that can disrupt the operation, functioning, integrity, or availability of a network or system.

War Dialing

These are the programs that automatically dial thousands of telephone numbers in search of a way in through a modem connection.

Buffer Overflow

It is a technique for crashing or gaining control of a computer by sending too much data to the buffer in a computer's memory. This is the type of DoS attack. Data sent to the server at the rate and volume that exceeds the capacity of the system, it will cause errors and damage the system.

Password Crackers

It is the software that can guess passwords. Password attacks can be implemented using several different methods like brute force attacks, Trojan horse programmers. IP spoofing can yield user accounts and passwords. Password attacks usually refer to repeated attempts to identify a user password or account.

Virus

A virus is a form of malicious code and as such is potentially disruptive. It may also be transferred unknowingly from one computer to another. Virus based attack manipulates the legitimate user to by authentication and access control mechanisms in order to execute the malicious code injected by the attacker. Virus attacks are often untargeted and spread among vulnerable systems and users. Virus attacks directly or indirectly decrease the availability of infected systems by consuming excessive amount of processing power or network bandwidth.

Types of Hackers

The different types of Hackers are

- White Hat Hackers
- Black Hat Hackers
- Blue Hat Hackers
- Spy Hackers

White Hat Hackers

White hat hackers are hackers who perform hacking for legitimate reasons. These are the good guys, computer security experts who specialize in penetration testing and other methodologies to ensure that a company's information systems are secure. These IT security professionals rely on a constantly evolving arsenal of technology to battle hackers.

Black Hat Hackers

These are the bad guys, who are typically referred to as just plain hackers. The term is often used specifically for hackers who break into networks or computers, or create computer viruses. Black hat hackers continue to technologically outpace white hats. They often manage to find the path of least resistance, whether due to human error or laziness, or with a new type of attack. Hacking purists often use the term "crackers" to refer to black hat hackers. Black hats' motivation is generally to get paid.

Blue Hat Hackers

A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch, looking for exploits so they can be closed. Microsoft also uses the term Blue hat to represent a series of security briefing events

Spy Hackers

Corporations hire hackers to infiltrate the competition and steal trade secrets. They may hack in from the outside or gain employment in order to act as a mole. Spy hackers may use similar tactics as hacktivists, but their only agenda is to serve their client's goals and get paid.

Cracking

The term "cracking" means trying to get into computer systems in order to steal, corrupt, or illegitimately view data. The popular press refers to such activities as hacking, but hackers see themselves as expert, elite programmers and maintain that such illegitimate activity should be called "cracking."

The term cracker was coined by Richard Stallman. Crackers are unauthorized users who attempt to obtain unauthorized access to remote systems. The nature of these attacks has changed substantially over the last few years. Several years ago crackers sat at terminal entering commands, waiting to see what would happen, and then entering commands. Today most cracking attacks are automated and take of attack is sometimes called an asymmetric attack.

Pornography

The growth of technology has flip side to it causing multiple problems in everyday life. Internet has provided a medium for the facilitation of crimes like pornography. Cyber porn as it is popularly called is widespread. Almost 50% of the web sites exhibit pornographic material on the Internet today. Pornographic materials can be reproduced more quickly and cheaply on new media like hard disks, floppy disks and CD-ROM's.

The new technology is not merely an extension of the existing forms like text, photographs and images. Apart from still pictures and images, full motion video clips and complete movies are also available. Another great disadvantage with a media like this is its easy availability and accessibility to children who can log on to pornographic web sites from their own houses in relative anonymity and social and legal deterrents associated with physically purchasing an adult magazine from the stand are no longer present.

Furthermore, there are more serious offences which have universal disapproval like child pornography and far easier for offenders to hide and propagate trough the medium of the internet.

Software Privacy

A term used to describe the act of illegally using, copying or distributing software without ownership or legal rights. The majority of software today is purchased as a one-site license, meaning that only one computer may have that software installed on it at one time. Copying that software to multiple computers or sharing it with your friend without multiple licenses is considered software privacy, which is illegal.

Computer programs are valuable property and thus the subject of theft from computer systems. Unauthorized copying of software is illegal because software is intellectual property that is protected by copy right law and user licensing agreement.

Software privacy is all but impossible to stop, although software companies are launching more and more lawsuits against major infractors. Originally, software companies tried to stop software privacy by copy-protecting their software. This strategy failed, however, because it was inconvenient for users and was not 100 percent foolproof. Most software now requires some sort of registration, which may discourage would-be pirates, but doesn't really stop software privacy.

An entirely different approach to software privacy called *shareware*. Shareware allows user to make copies for others and public domain software, which is not copyrighted. Shareware publishers encourage users to give copies of programs to friends and colleagues but ask everyone who uses a program regularly to pay a registration fee to the program's author directly.

Data recovery

Data recovery is the process of handling the data; through the data is damaged, failed, corrupted or cannot accessible from secondary storage media then it cannot be accessed normally. The data are being kept in storage media such as internal or external hard disk drives, pen drive, storage tapes, CDs, DVDs etc. Recovery is needed due to physical damage to the storage device or logical damage to the file system that prevents it from being mounted by the host operating system (OS).

The most common data recovery scenario involves an operating system failure, accidental damage etc; in such case copy all wanted files to another disk. This can be easily done by using a CD or pen drives. In order to move the files from the system disk to the backup media file manager or optical disc authoring software is used.

In case of hard disk failure, the data cannot be easily read. The solutions are repairing the file system, hard disk recovery techniques to recover the corrupted data, hardware-software based recovery of damaged service areas to hardware replacement on a physically damaged disk. If the Files erased, then the contents of deleted files are not removed immediately from the drive; instead, references to them in the directory structure are removed, and the space they occupy is made available for later overwriting. For the end users, deleted files are not discoverable through a standard file manager, but that data still technically exists on the drive. In the meantime, the original file contents remain, often in a number of disconnected fragments, and may be recoverable. The Data recovery process is also used in forensic applications.

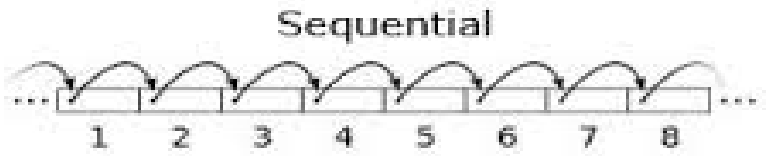
File Modification and File Access

File is a collection of related data records treated as a unit. It is also called as Data set. A computer file is organized in a particular way with a well defined structure. File management controls the processes such as file creation, deletion and access.

Files reside on secondary storage. When we want to use this information, it has to be accessed and brought into main memory. Information in files could be accessed in many ways. This depends on an application used. There are three file access methods.

Sequential Access

It is a simple access method. All the records are kept in some sequence such as numerical order. Records in this type of file are located one after another according to the given order. The information in a file is accessed sequentially one record after another. Sequential access is based on the tape model that is inherently a sequential access device. Sequential access is best suited where most of the records in a file are to be processed. For example, transaction files.

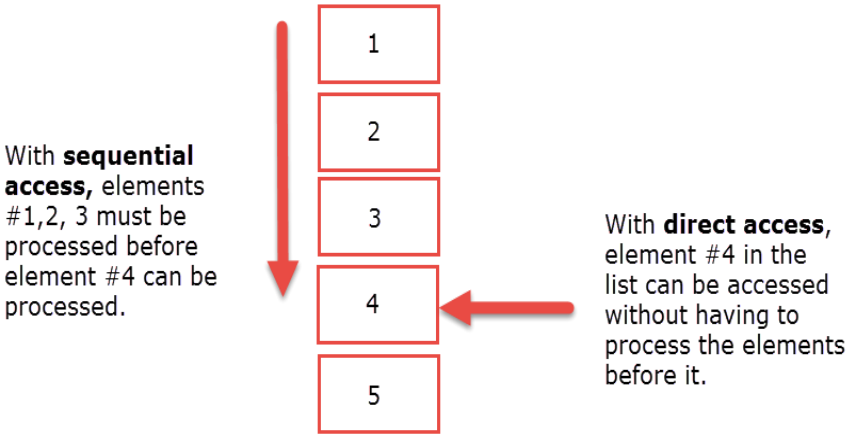


Direct Access

Direct access file uses a physical medium and programming, which helps in the storage and retrieval of specific records. These files are the heart of DBMS and most of today's file storage technology. Sometimes it is not necessary to process every record in a file. It may not be necessary to process records in the order in which they are present. Most common device for storing direct access files is magnetic disk.

Information present in a record can be accessed only if some key value in that record is known. In all such cases, direct access is used. A file is a collection of physical blocks, and so the records in any block can be accessed. For example, master files.

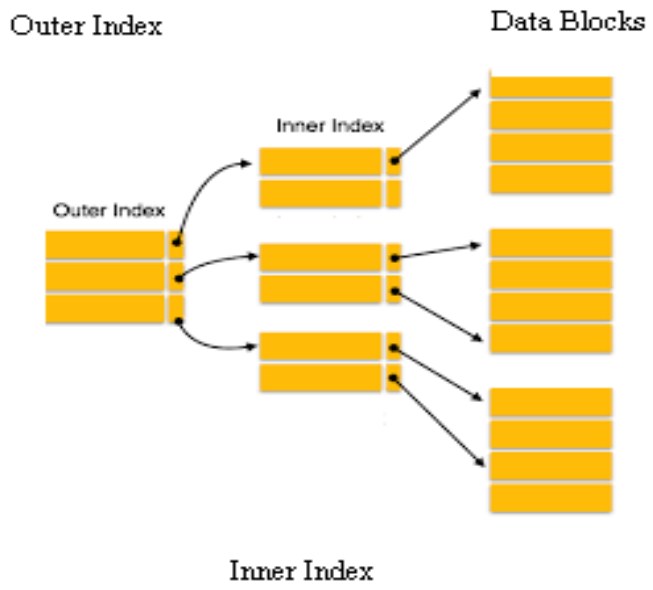
Databases are of this type since they allow query processing that involves immediate access to large amounts of information. Not all operating systems support direct access files. Usually files are to be defined as sequential or direct at the time of creation and accessed accordingly later. All reservation systems fall into this category.



Indexed Sequential Access

This access method is a slight modification of the direct access method. It is a combination of both the sequential access as well as direct access. The main concept is to access a file direct first and then sequentially from that point onwards. This access method involves maintaining an index. The index is a pointer to a block. To access a record in a file, a direct access of the index is made. The information obtained from this access is used to access the file. For example, the direct access to a file will give the block address and within the block the record is accessed sequentially. Sometimes indexes may be big. So hierarchies of indexes are

built in which one direct access of an index leads to info to access another index directly and so on till the actual file is accessed sequentially for the particular record. The main advantage in this type of access is that both direct and sequential access of files is possible.



Recover Internet Usage Data

Recovery experts do not always need to have physical access to the damaged hardware. When the data is lost; then it can be recovered by using software techniques. It can perform the recovery process by using remote access software over the Internet or other connection to the location of the lost or damaged data. Remote recovery requires an internet connection with an adequate bandwidth.

Methodology that helps in Remote Data recovery are:

Logical recovery of files & partition

After the drive has been ready to use, it is possible the retrieve the lost data. If the drive has failed logically, there are a number of reasons for that. User can repair the files in order to read the file system's data structure and retrieve stored data.

Repair the damaged files can be retrieved

Data loss or damage may occur when, for example, a file is written to a sector on the drive that has been damaged. Corrupted documents can be recovered by several software methods or by manually reconstructing the document using a hex editor.

Recover Swap File

Swap file is a file stored on the computer hard drive that is used as a temporary location to store information that is not currently being used by the computer RAM. By using a swap file a computer has the ability to use more memory than what is physically installed in the computer.

It is useful technique that enables a computer to execute programs and manipulate files larger than main memory. The operating system copies as much data as possible into main memory, and leaves the rest on the disk. The least recently used files in RAM can be "swapped out" to hard disk until they are needed. New files can be "swapped in" to RAM. In larger operating systems the units that are moved are called pages and the swapping is called paging.

Swap files are used in operating systems like Windows 7 and Windows Server 2008, as virtual memory is a cheaper alternative to magnetic media. A typical swap file is equal to or larger than the system's total installed physical memory. Although swap files provide additional system memory, the data stored in swap files is typically less active and idle. The swap files can

be corrupted due to raw partition, virus attacks or system crash. User can get back the corrupted files by using the recovery tools. These recovery tools helps in the maintenance of swap file data in a secured way.

Recover Temporary Files

Deleted files are inaccessible. We can often recover them completely with professional data recovery tools. Data recovery software is designed to locate any recoverable data and providing it in a proper format. The best data recovery applications provide a preview of recovered files, filtered and searchable results and easy file restoration

File recovery programs can be used to save files of any type or size, from pictures, music and videos to documents and spreadsheets. Data recovery software can locate and restore emails, executables and compressed files. The best file recovery software can even maintain the folder organization of your files, and it may be able to recover a complete partition or drive.

Recover Cache Files

A cache is a place to store something temporarily in a computing environment. The active data is often cached to shorten data access times, reduce latency and improve input/output. Because almost all application workload is dependent upon I/O operations, caching is used to improve application performance.

The web browsers such as Internet Explorer, Firefox and Chrome use a browser cache to improve performance for frequently accessed web pages. When you visit a webpage, browser requests are stored on computing storage in the browser's cache. If you click "back" and return to that page, your browser can retrieve most of the files it needs from cache instead of requesting they all be sent again. This approach is called read cache. It is much faster for your browser to read data from the browser cache than to have to re-read the files from the web page.

Types of cache

Write-around cache

It allows write operations to be written to storage, skipping the cache altogether. This keeps the cache from becoming flooded when large amounts of write I/O occur. The disadvantage is that data is not cached unless it is read from storage. As such, the initial read operation will be comparatively slow because the data has not yet been cached.

Write-through cache

It writes data to both the cache and storage. The advantage to this approach is that newly written data is always cached, thereby allowing the data to be read quickly. A drawback is that write operations are not considered to be complete until the data is written to both the cache and primary storage. This causes write-through caching to introduce latency into write operations.

Write-back cache

It is similar to write-through caching in that all write operations are directed to the cache. The difference is that once the data is cached, the write operation is considered complete. The data is later copied from the cache to storage. In this approach, there is low latency for both read and write operations. The disadvantage is that, depending on the caching mechanism used, the data may be vulnerable to loss until it is committed to storage.

Steps to retrieve the cache files from different browsers:

Retrieve temporary Internet files from Internet Explorer versions 7 and 8.

- ✓ Access and open Internet Explorer through your Start menu or by clicking on the icon directly from your desktop. Click on Tools, then on Internet Options. Click on the General tab and then click on Settings under the Browsing History section. In Settings, click on View Files to retrieve and view your temporary Internet files.

Retrieve temporary Internet files from Internet Explorer 6.

- ✓ Access and open Internet Explorer through your Start menu or by clicking on the icon directly from your desktop. Click on Tools, then on Internet Options. Click on the

General tab and then click on Settings under the Temporary Internet Files section. In Settings, click on View Files to retrieve and view your temporary Internet files

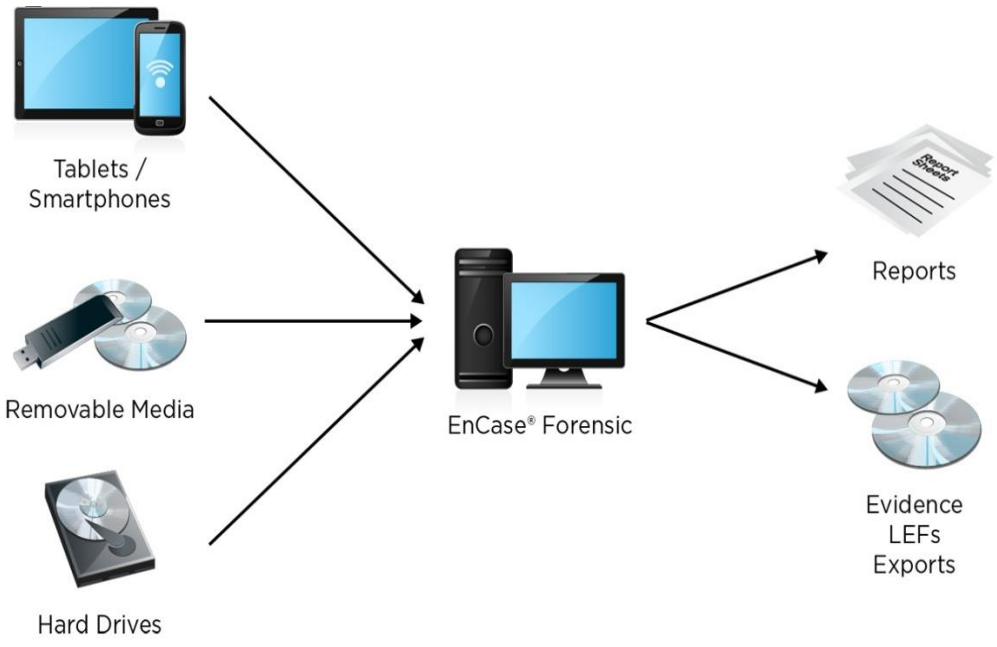
Retrieve temporary Internet files from Google Chrome.

- ✓ Type "about:cache" directly into the address bar of Google Chrome. Your temporary Internet files, or cache content, will then be displayed in the browser window. Depending on how full your cache is, the data may take a few moments to display.

Introduction to Encase Forensic

Encase Forensic provides investigators with a single tool for conducting large-scale and complex investigations from beginning to end. One of the most powerful features of Encase Forensic is its ability to organize different types of media together, so that they can be indexed and searched as a unit rather than individually. It is the global standard in digital investigation technology for forensic practitioners who need to conduct efficient, forensically-sound data collection and investigations using a repeatable and defensible process.

The word “forensics” comes from Latin word forensic, which in the time of the Romans referred to the public forum. When an organization’s information resources have been interfered with in the course of an incident, and the organization decides to apprehend and prosecute the offender, it must collect information in such a way that it will be usable in a criminal or civil proceeding. This information is usually called “evidence”, but in fact nothing is evidence until a judge admits it as such in court. During legal proceedings, opposing can challenge this admission on every available ground. Even something as simple as just taking a look at a compromised computer may allow opposing counsel to challenge the information gathered from that computer on the grounds that it might have been modified.



When setting out to plan for an organization commitment to forensic operations, you should consider the following:

i) Cost
ii) Response Time
iii) Data sensitivity concerns

Costs:

This will include costs such as those for the tools, hardware and other equipment used to collect and examine digital information, as well as for staffing and training.

Response Time:

While an outside forensic consultant may seem cheaper because the service is only paid for when actually used, the interruption to normal business operations while the consultant gets into place and up to speed may turn out to be more expensive than maintaining an in-house forensic capability.

Data sensitivity concerns:

Forensic data collection can expose highly sensitive information such as personal health records, credit card information, business plans etc.

Resolving these issues can be challenging, so many organizations divide the forensic functions as follows:

i) First Response
ii) Analysis and presentation

First Response:

It is used for identifying the sources of relevant digital information and preserving it for later analysis, using sound process.

Analysis and presentation:

Analyzes the collected information to identify material facts that bear on the subject of the investigation and prepares and presents the results of the analysis to support possible legal action.

Firewalls

A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Need of Firewalls

Without a firewall, your computer is operating with an "open door" policy. Bank account information, passwords, credit card numbers, virtually any sensitive information on your computer becomes available to hackers. Hackers can get in, take what they want, and even leave one of their own "back doors" in place for ongoing access to your computer whenever they like.

Firewalls have a wide range of capabilities.Types of firewalls include:

- Packet filtering firewalls
- Stateful inspection firewalls
- Proxy firewalls
- Guards
- Personal firewalls

Packet filter

Packet filtering is “controlling access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination. Packet filtering is one technique, among many, for implementing security firewalls.”i Packet filtering is both a tool and a technique that is a basic building block of network security. It is a tool in that it is an instrument that aids in accomplishing a task. It is a

technique because it is a method of accomplishing a task. In the context of a TCP/IP network, a packet filter watches each individual IP datagram, decodes the header information of in-bound and out-bound traffic and then either blocks the datagram from passing or allows the datagram to pass based upon the contents of the source address, destination address, source port, destination port and/or connection status. This is based upon certain criteria defined to the packet filtering tool. The leading IP routers, including Cisco, Bay, and Lucent, can be configured to filter IP datagrams. Many operating systems can be configured for packet filtering. Packet filtering can be added to *nix operating systems. Support for packet filtering via ipchains is included by default in the Linux kernel. Windows NT and Windows 2000 support packet filtering. Virtually all commercial firewalls support packet filtering. Some commercial firewalls also have the capability of filtering packets based upon the state of previous packets (stateful inspection).

Purpose of Packet Filter

Packet filtering generally is inexpensive to implement. However it must be understood that a packet filtering device does not provide the same level of security as an application or proxy firewall. All except the most trivial of IP networks is composed of IP subnets and contain routers. Each router is a potential filtering point. Because the cost of the router has already been absorbed, additional cost for packet filtering is not required. Packet filtering is appropriate where there are modest security requirements. The internal (private) networks of many organizations are not highly segmented. Highly sophisticated firewalls are not necessary for isolating one part of the organization from another. However it is prudent to provide some sort of protection of the production network from a lab or experimental network. A packet filtering device is a very appropriate measure for providing isolation of one subnet from another.

Functionality

All packet filters function in the same general fashion. Operating at the network layer and transport layer of the TCP/IP protocol stack, every packet is examined as it enters the protocol stack. The network and transport headers are examined closely for the following information:

protocol (IP header, network layer) – In the IP header, byte 9 (remember the byte count begins with zero) identifies the protocol of the packet. Most filter devices have the capability to differentiate between TCP, UPD, and ICMP.(TCP-Transmission Control Protocol,UDP-User Datagram Protocol,Internet Control Message Control)

source address (IP header, network layer) – The source address is the 32-bit IP address of the host which created the packet.

destination address (IP header, network layer) – The destination address is the 32-bit IP address of the host the packet is destined for

source port (TCP or UDP header, transport layer) – Each end of a TCP or UDP network connection is bound to a port. TCP ports are separate and distinct from UDP ports. Ports numbered below 1024 are reserved – they have a specifically defined use. Ports numbered above 1024 (inclusive) are known as ephemeral ports. They can be used however a vendor chooses. For a list of "well known" ports, refer to RFP1700. The source port is a pseudo-randomly assigned ephemeral port number. Thus it is often not very useful to filter on the source port.

destination port (TCP or UDP header, transport layer) – The destination port number indicates a port that the packet is sent to. Each service on the destination host listens to a port. Some well-known ports that might be filtered are 20/TCP and 21/TCP - ftp connection/data, 23/TCP - telnet, 80/TCP - http, and 53/TCP - DNS zone transfers.

connection status (TCP header, transport layer) – The connection status tells whether the packet is the first packet of the network session. The ACK bit in the TCP header is set to "false" or 0 if this is the first packet in the session. It is simple to disallow a host from establishing a connection by rejecting or discarding any packets which have the ACK bit set to "false" or 0.

The filtering device compares the values of these fields to rules that have been defined, and based upon the values and the rules the packet is either passed or discarded. Many filters also

allow additional criteria from the link layer to be defined, such as the network interface where the filtering is to occur.

Types of Packet Filtering

Packet filtering firewall allows only those packets to pass, which are allowed as per your firewall policy. Each packet passing through is inspected and then the firewall decides to pass it or not. The packet filtering can be divided into two parts:

1. Stateless packet filtering.
2. Stateful packet filtering.

The data travels through the internet in the form of packets. Each packet has a header which provides the information about the packet, its source and destination etc. The packet filtering firewalls inpects these packets to allow or deny them. The information may or may not be remembered by the firewall.

Stateless Packet Filtering

If the information about the passing packets is not remembered by the firewall, then this type of filtering is called stateless packet filtering. This type of firewalls are not smart enough and can be fooled very easily by the hackers. These are especially dangerous for UDP type of data packets. The reason is that, the allow/deny decisions are taken on packet by packet basis and these are not related to the previous allowed/denied packets.

Stateful Packet Filtering

If the firewall remembers the information about the previously passed packets, then that type of filtering is stateful packet filtering. These can be termed as smart firewalls. This type of filtering is also known as Dynamic packet filtering.

Stateful Inspection Firewall

Stateful Inspection Firewall is a firewall that keeps track of the state of network connections traveling across it.

Functionality

Firewall protection uses stateful inspection to track current connections. Stateful inspection tracks source and destination IP addresses, ports, applications, and other connection information. Before the client inspects the firewall rules, it makes the traffic flow decisions that are based on the connection information.

For example, if a firewall rule allows a computer to connect to a Web server, the firewall logs the connection information. When the server replies, the firewall discovers that a response from the Web server to the computer is expected. It permits the Web server traffic to flow to the initiating computer without inspecting the rule base. A rule must permit the initial outbound traffic before the firewall logs the connection.

Stateful inspection eliminates the need to create new rules. For the traffic that is initiated in one direction, you do not have to create the rules that permit the traffic in both directions. The client traffic that is initiated in one direction includes Telnet (port 23), HTTP (port 80), and HTTPS (port 443). The client computers initiate this outbound traffic; you create a rule that permits the outbound traffic for these protocols. Stateful inspection automatically permits the return traffic that responds to the outbound traffic. Because the firewall is stateful in nature, you only need to create the rules that initiate a connection, not the characteristics of a particular packet. All packets that belong to an allowed connection are implicitly allowed as being an integral part of that same connection.

Stateful inspection supports all rules that direct TCP traffic. Stateful inspection does not support the rules that filter ICMP traffic. For ICMP traffic, you must create the rules that permit the traffic in both directions. For example, for the clients to use the ping command and receive replies, you must create a rule that permits ICMP traffic in both directions.

The state table that maintains the connection information may be periodically cleared. For example, it is cleared when a Firewall policy update is processed or if Symantec Endpoint Protection services are restarted.

Proxy Firewalls

A Proxy is a central machine on the network that allows other machines in that network to use a shared Internet connection. Proxy servers are intermediate servers which accept requests from clients and forward them to other proxy servers, a source server, or service the request from their own cache. The proxy is also called 'server' or 'gateway'. Proxy allows users on a network to browse the Web, send files over FTP, and work with E-mail and other Internet services.

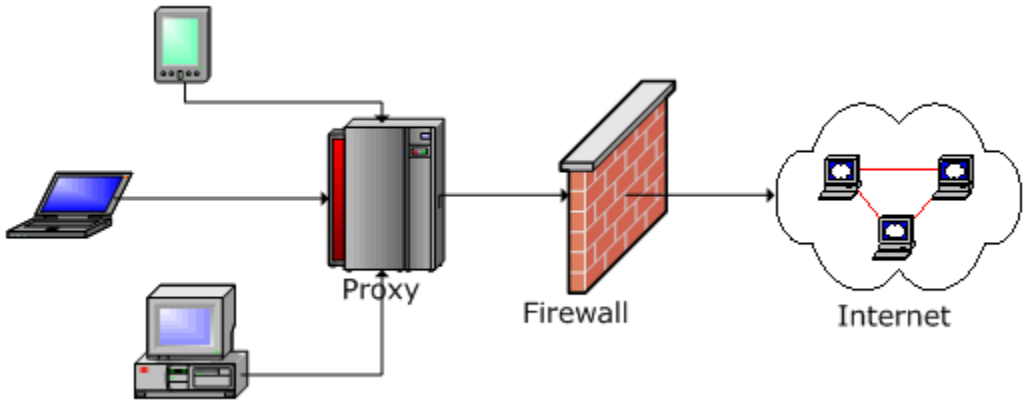
A Firewall Proxy provides Internet access to other computers on the network but is mostly deployed to provide safety or security. It controls the information going in and out the network. Firewalls are often used to keep the network safe and free of intruders and viruses. Firewall proxy servers filter, cache, log, and control requests coming from a client. A firewall proxy is one that is used for restricting connections from a proxy to the outside world or to the source server inside of the LAN. This is different from a conventional firewall, in that a conventional firewall restricts connections coming from the outside world.

Functionality

Simply put, proxy are gateway applications used to route Internet and web access from within a firewall. Proxy servers work by opening a socket on the server and allowing the connection to pass through. There is often only one computer in a company with direct Internet connection. Other computers have access to the Internet using that computer as gateway.

A proxy basically does the following:

1. Receives a request from a client inside the firewall
2. Sends this request to the remote server outside of the firewall
3. Reads the response
4. Sends it back to the client



Usually, the same proxy is used by all of the clients on the network. This enables the proxy to efficiently cache documents that are requested by several clients.

SOCKS4 or SOCKS5 Proxy

In a SOCKS network, all network application data flows through SOCKS, enabling SOCKS to collect, audit, screen, filter and control the network data, and create a network application data warehouse.

It is recommended to use SOCKS5 proxy with PostCast Server. SOCKS4 performed three functions: connection request, proxy server setup and application data relay. SOCKS5 brings authentication to the table. With authentication, SOCKS5 adds two messages. SOCKS5 makes configuring clients easier and includes support for UDP and TCP applications such as SNMP and

audio/video applications such as RealAudio. It supports communications among networks with different IP addressing schemes, and supports authentication and encryption.

Tunneling Proxy

Tunneling allows users to perform various Internet tasks despite the restrictions imposed by firewalls. This is made possible by sending data through HTTP (port 80). Additionally, Tunneling protocol is very secure, making it indispensable for both average and business communications. SSL (Secure Sockets Layer) tunneling protocol allows a web proxy server to act as a tunnel for SSL enhanced protocols. The client makes an HTTP Request to the proxy and asks for an SSL tunnel. A Tunneling Proxy operates on port 443.

Guard

In information security, a guard is a device or system for allowing computers on otherwise separate networks to communicate, subject to configured constraints. In many respects a guard is like a firewall and guards may have similar functionality to a gateway.

Whereas a firewall is designed to limit traffic to certain services, a guard aims to control the information exchange that the network communication is supporting at the business level. Further, unlike a firewall a guard provides assurance that it is effective in providing this control even under attack and failure conditions.

A guard will typically sit between a protected network and an external network, and ensure the protected network is safe from threats posed by the external network and from leaks of sensitive information to the external network.

A guard is usually dual-homed, though guards can connect more than two networks, and acts as a full application layer proxy, engaging in separate communications on each interface. A guard will pass only the business information carried by the protocols from one network to another, and then only if the information passes configured checks which provide the required protection.

Guards were initially designed to control the release of information from classified systems, protecting the confidentiality of the sensitive information handled by the protected system. Since then their scope has been extended to cover controls over the import of data, in order to protect the integrity of information and availability of services in the protected network.

Guards generally provide the following functionality:

- source and destination address authentication
- source and destination address whitelisting
- security label checks against source and destination clearances
- data format whitelisting
- data format consistency and validity checking
- scanning data for known malware
- validation of digital signatures
- inspection of encrypted content
- checking text against a blacklist of phrases
- removal of redundant data
- generation of logs recording security relevant events
- self-test mechanisms

Personal firewall

A personal firewall is an application which controls network traffic to and from a computer, permitting or denying communications based on a security policy. Typically it works as an application layer firewall.

A personal firewall differs from a conventional firewall in terms of scale. A personal firewall will usually protect only the computer on which it is installed, as compared to a conventional firewall which is normally installed on a designated interface between two or more networks, such as a router or proxy server. Hence, personal firewalls allow a security policy to

be defined for individual computers, whereas a conventional firewall controls the policy between the networks that it connects.

The per-computer scope of personal firewalls is useful to protect machines that are moved across different networks. For example, a laptop computer may be used on a trusted intranet at a workplace where minimal protection is needed as a conventional firewall is already in place, and services that require open ports such as file and printer sharing are useful. The same laptop could be used at public Wi-Fi hotspots, where strict security is required to protect from malicious activity. Most personal firewalls will prompt the user when a new network is connected for the first time to decide the level of trust, and can set individual security policies for each network.

Unlike network firewalls, many personal firewalls are able to control network traffic allowed to programs on the firewalled computer. When an application attempts an outbound connection, the firewall may block it if blacklisted, or ask the user whether to blacklist it if it is not yet known. This protects against malware implemented as an executable program. Personal firewalls may also provide some level of intrusion detection, allowing the software to terminate or block connectivity where it suspects an intrusion is being attempted.

Common personal firewall features:

- Block or alert the user about all unauthorized inbound or outbound connection attempts[1]
- Allows the user to control which programs can and cannot access the local network and/or Internet and provide the user with information about an application that makes a connection attempt
- Hide the computer from port scans by not responding to unsolicited network traffic
- Monitor applications that are listening for incoming connections
- Monitor and regulate all incoming and outgoing Internet users
- Prevent unwanted network traffic from locally installed applications
- Provide information about the destination server with which an application is attempting to communicate

Authentication and Access Control:

Identification

Identification is nothing more than claiming you are somebody. You identify yourself when you speak to someone on the phone that you don't know, and they ask you who they're speaking to. When you say, "I'm Jason.", you've just identified yourself.

In the information security world, this is analogous to entering a username. It's **not** analogous to entering a password. Entering a password is a method for verifying that you are who you identified yourself as, and that's the next one on our list.

Identification is the means by which a user provides a claimed identity to the system.The most common form of identification is the user ID.

There are ways of authenticating a user's identity.

1.Proof by knowledge,e.g.(password)

2.Proof by possession,e.g.(pincard)

3.Proof by property(biometrics),e.g.(fingerprint)

Proof by Knowledge

A password is associated with each user or entity.Password are shared secrets between user and system.To gain access to the system,the user enters a user ID and password.The system authenticates the user if the password matches with that stored in the system corresponding to user ID.There are different ways to store passwords in the system.

Clear passwords: The system stores passwords in clear text in clear text in password file,which is 'read'and 'write' protected form users.It provides no protection from system administrator or super

user.Stroage of password files on backup media also poses security risk.

Encrypted password:A one-way functions of passwords are stored instead of clear passwords.When a user enters the password,the system computers one-way function of the password and compares with that stored in the system.

Threats on Passwords

Replay: An adversary records the password when it is transmitted in clear text over the communication line.The recorded password is subsequently used to impersonate.

Brute-force attack: An adversary tries all possible passwords,one at a time in the hope to uncover the correct password.The feasibility of the attack depends on number of trials required and the time taken for each trial.

Password guessing: The adversary guesses the passwords by trying names of user's family members or proper names.

Dictionary attacks: The adversary tries to match the password with dictionary words.Apart from standard dictionary,one line dictionaries of words from forewign languages,specialized words from music and flims are also available.Dictionary attack is generally not successful on a single user's password,but it may uncover a weak password to gain access to system.

Safeguards

a) Password rules are imposed to prevent use of weak password such as:
   _Minimum length of passwords and allowable set of characters,uppercase,numeric,non-alphanumeric are specified.
   --The password ageing time frames are specified to enforce change in passwords.

   _Generations of expired passwords being disallowed for use are specified.
b) A site may use reactive password checking strategy in which password cracker programmer is run periodically to find weak passwords.
c) A site may use proactive password checking scheme in which the system checks for all allowable password at the time of registration.If the password is weak,it is rejected.

Proof by Possession

A user presents physical token that the system can recognize as belonging to him such as a banking card,smart card or ATM card.Personal Identification Numbers are often used along with physical token to identify the user.To prevent brute force attack on PIN,the machine-confiscate the card by locking it and deactivates it if three unsuccessful attempts are made to enter the PIN.

PINs are second level of security in case the card is lost or stolen.However,since users often do not keep the two things separate,theft is a regular occurrence in this case.

Proof by Property

Biometric techniques relay on measuring readily accessible and reliable unique characteristics of users such as fingerprints,written signatures,voice patterns,retinal scans,face geometry and hand geometry.When the system needs to authenticate the user,the system obtains a biometric measure of the user and then compares it against that stored in the database.

Authentication

Authentication is the process of determining if a user or identity is who they claim to be. Authentication is accomplished using something the user knows (e.g. password), something the user has (e.g. security token) or something of the user (e.g. biometric).

The authentication process is based on a measure of risk. High risk systems, applications and information require different forms of authentication that more accurately confirm the user's digital identity as being who they claim to be than would a low risk application, where the confirmation of the digital identity is not as important from a risk perspective. This is commonly

referred to as "stronger authentication".

Authentication processes are dependant upon identity verification and registration processes. For example, when Jane Doe is hired at an enterprise, she provides the enterprise with information and tokens of who she is (e.g. name, address, driver's license, birth certificate, a SSN number, a passport, etc.). The enterprise may choose to immediately accept this information or, it may instead chose to run background checks on Jane to see if she is who she claims to be and determine if she has any criminal record. When the checks come back favorably, the enterprise will accept her identity and enter her into their systems. The identity registration process will usually involve issuing Jane with enterprise authentication mechanisms such as id and password, security token, digital certificate and/or registering some of her biometrics.

The authentication process is totally dependent on the identity validation and registration process used for Jane. If Jane presents false tokens, which are accepted by the enterprise, then the person acting as Jane will be positively authenticated every time, even though she is not the real Jane Doe. Authentication security therefore is only as good as the weakest link in the chain.

General Authentication

Password Authentication

Password authentication is the most common method of authentication. It is also the least secure. Password authentication requires the identity to input a user id and a password in order to login. Password length, type of characters used and password duration are password management are now critical concern in enterprises. The ability to easily crack passwords has resulted in high levels of identity theft. As a result, the high risk of passwords means most enterprises now deploy a layered security strategy. A user enters in their id and password for initial login to gain access to only low risk information and applications with other forms of authentication required for higher risk information and applications.

Single Sign On Authentication

Single Sign On (SSO), Reduced Sign On (RSO), or Enterprise Single Sign On (ESSO) is the ability to reduce the number of id's and passwords a user has to remember. In most enterprises, a strong business case can be made to implement single sign on by reducing the number of password related help desk calls. SSO is also the architecture to require stronger forms of authentication for higher risk information and applications. Thus a user may login using their id and password to gain general low risk access to an enterprise. The SSO software enables them to not have to use multiple id's and passwords. However, when the user tries to access more sensitive information and applications, the single sign on software will require the identity to input stronger authentication such as a security token, a digital certificate and/or a biometric.

Lightweight Directory Access Protocol (LDAP) Authentication

Most enterprises use Lightweight Directory Access Protocol (LDAP) directories to handle the centralized authentication. LDAP directories, such as Active Directory, Sun One Directory, Novel e-Directory and other vendors, provide a low cost way of doing fast identity look-ups and authentication as compared to traditional databases. Today it is also common to use virtual LDAP directories to quickly integrate the identity and authentication information contained in one or more databases and/or other LDAP directories. The use of these directories is a critical piece of identity infrastructure that leads to integrating access control.

Access Control Authentication

Access control is the process of granting an identity the ability to physically or electronically access a facility or enterprise. By using LDAP directories and single sign on, many enterprises now integrate their building access control security cards, employee time keeping and other access control accessories into their LDAP identity management system. This reduces the number of identity database silos, since most access control systems use their own identity databases. It also reduces the number of access control accessory systems.

Network Authentication

Network authentication is the process of granting an identity the ability authenticate to a network as well as their authorization. Almost all network authentication systems are now LDAP based. This includes Microsoft 2000, Linux, Solaris, AIX and HPUX. Many mainframe authentication systems such as RACF are now LDAP enabled.

Biometric Authentication

Biometric authentication s is the process of taking a "piece of you", digitizing it and then using this to authenticate against an identity directory or database. Typical types of biometric authentications include finger scans, digital finger prints, hand scans, retina scans, digital signature scans and others. The use of DNA biometrics is increasingly used in identity verification (the initial identity registration step prior to authentication). Biometrics are commonly used as part of an array of authentication methods used in enterprises.

Strong Authentication

Strong authentication means higher trust of an authentication. For instance, the successful login using a id and password will be given a low level of trust by the enterprise since the id and password are easily obtained by social engineering or password cracking. Stronger authentication methods include digital certificates, security tokens and biometrics. Often, many enterprises use combinations of these including passwords, to place a higher degree of trust for higher risk applications or information access.

Transaction Authentication

Transaction authentication is the process of using other authentication determinants to verify an identity. Often used by financial institutions for higher risk customers or transactions, the transaction software looks at the IP address the user is coming in on, the identity's computer hardware they're using, the time of day, the geo-location the identity is coming from, etc. If the identity successfully logs on using a id and password BUT the other components are not usual, the transaction authentication software may stop a process, flag in real time an administrator and/or ask the user more questions to have more confidence the identity is who they claim to be.

Federated Authentication

Federated authentication is the ability to trust an incoming electronic identity to the enterprise from a trusted partner or website. Protocols enabling this include SAML, Liberty Alliance, Web Services Federation and Shibboleth. When combined with enterprise single sign on systems, the user experience is improved since they no longer have to remember another id and password. Further, enterprise identity authentication standards can be automatically enforced on external identities using the enterprise systems. Identity authentication federation also works in reverse for enterprise employees who access there 401k, benefits, etc, to outside supplier websites. By using federated authentication, the identity doesn't need to remember another separate id and password.

PKI Authentication

Public key infrastructure (PKI) authentication, is another way of doing identity authentication. An identity is given a digital certificate by an Certificate Authority (CA). This is then presented during the authentication process to verify an identity is who they say they are. The level of authentication trust varies for digital certificates depending on the level of identity verification done during the identity registration process as well as the digital certificate revocation process. Digital certificates are becoming more important to authenticate and verify an identity in single sign on systems, document management systems and in web services.

Security Token Authentication

Security token authentication, such as RSA secureID tokens, are used to authenticate an identity (something that you have). During the login process, or if required by a single sign on system for a higher risk application, the identity is required to enter in the numbers appearing on

the token screen along with their id. Since the numbers change randomly to the user viewing the screen (but is understood by the central authentication server), there is a higher degree of trust associated with this form of authentication. However, operating costs for security authentication tokens are higher than the use of password and id since they must be physically issued, replaced and recovered.

Smart Card Authentication

Smart cards are another form of authentication token (something you have). Often they contain a digital certificate as well as additional identity attribute information. Smart card authentication is becoming wide spread. The same smart cards used in an authentication process are now commonly used as well for access control mechanisms to enter physical facilities, buildings, floors and rooms.

Authentication Management

Authentication management is the overall process of managing identities and their authentication mechanisms. In most enterprise authentication management involves authentication policies and processes to manage passwords, digital certificates, security tokens, access control, biometrics, smart cards, LDAP directories, transaction authentication, single sign on and identity authentication federation. Strong business cases can be made to lower authentication costs while at the same time strengthening overall enterprise security.

Wireless Authentication

Authenticating wireless devices is today becoming a main enterprise security issue. Often, the authentication used is very insecure or easily breached. There are however ways to increase reliability that the user is who they claim to be by using multi-factor authentication.

Document Authentication

Formely separate document authentication systems are now becoming intertwined with enterprise identity and authentication mechanisms. Gone are the days of relying upon mostly passwords to authenticate users trying to open document. Formerly separate document authentication systems are now becoming intertwined with enterprise identity and authentication mechanisms. Gone are the days of relying upon mostly passwords to authenticate users trying to open documents.

Outsourcing Authentication

Many modern enterprises have outsourced portions of their authentication development, maintenance and troubleshooting. If done well it can save the enterprise money. If done poorly, it can create security holes or, cause enterprise failures.

Firewalls implement the authentication process:

Most operating systems are equipped with authentication schemes.Web servers can be configured to authenticate clients who want to access certain protected content.Firewalls,too,can perform user authentication.In fact,many organizations depend on firewalls to provide more secure authentication than conventional systems.Authentication is a key function because firewalls exist to give external users access to protected resources.

A firewalls uses authentication to identify individuals so that it can apply rules that have been associated with those individuals.Some firewalls use authentication to give employees access to common resources such as the web or file transfer protocol(FTP).Some identify the user associated with a particular IP address;after the user is authorized,the IP address can then be used to send and receive information with hosts on the internal network.

The exact steps that firewalls follow to authenticate users may vary,but the general process is the same:

1. Client makes request to access a resource
2. Firewall intercepts the request and prompts the user for name and password
3. User submits information to firewall

4. User is authenticated
5. Request is checked against firewall's rule base
6. If request matches existing allow rule, user is granted access
7. User accesses desired resources

The "plain English"version of the exchange between external client and authenticating firewall is illustrated in figure

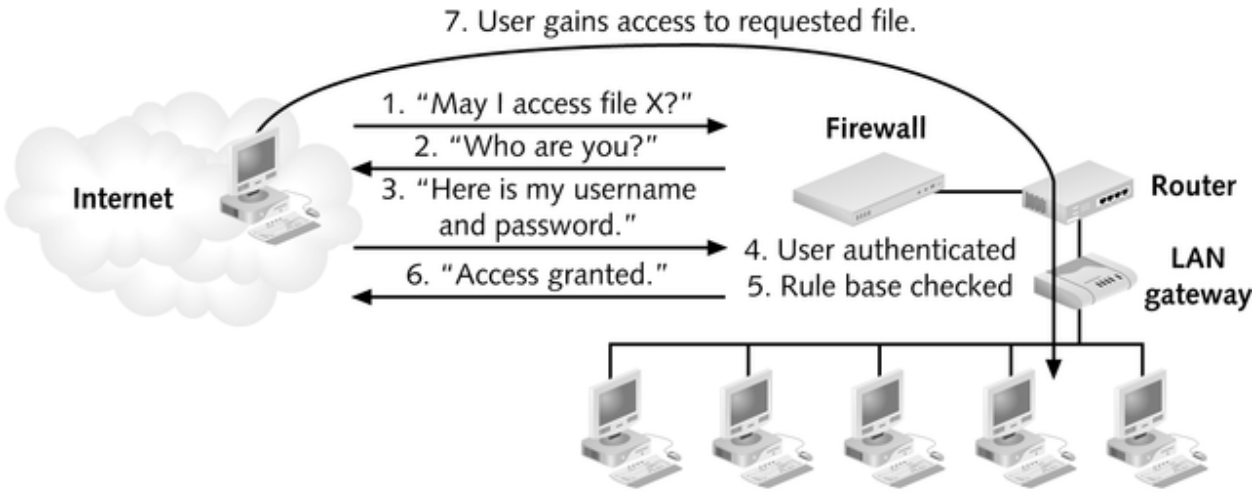


Figure 6-1 Basic external user authentication

Strong Authentication

Passkeys: User password is mapped to a one-way has-function to generate a cryptographic key. Such password-derived keys are known as passkeys.The passkey is used to secure communication link between user and the system.

One time passwords:A special equipment generates a pseudorandom number which is used as password.The password is changed every minute and is time synchronized to the database stored in the computer.This method is expensive because of the additional hardware.

Challenge response protocol:In proof of knowledge method using passwords,the user discloses the passwords to prove the knowledge of the shared secrete.Whereas,in the challenge-response method,a user provides his/her identity by responding correctly to the challenge asked by the verifier.For example,the user and the system agree on function f=x2+5.when the user logs in,the system randomly selects a number say 10 and sends it to user,the user has to reply with number 105 for valid authentication.

Protected Password

A strong password is one that's hard to crack. A strong password must have all of the following:

- Your password must be no fewer than eight (8) characters in length. **However, a good choice is a "pass phrase" composed of four (4) words and punctuation.** A pass phrase is a longer version of a password and is therefore more secure. A pass phrase is typically composed of multiple words.
  - Note: Though technology constraints may impose maximum length or other restrictions, use of pass phrases shall be supported where possible and practical.
  - Examples of pass phrases:
    - I like ice cream.
    - Turn Off Cell Phones!
    - It was hot today.

    - Cal Poly Broncos rule!
- At least three of the following four types of characters:
    - It must have at least one number.
    - It must have at least one uppercase letter.
    - It must have at least one lowercase letter.
    - It must have at least one symbol (!,@,#,$,^).

Examples of Extremely Bad Passwords

- Your name in any form - first, middle, last, maiden, spelled backwards, nickname or initials
- Your user ID or your user ID spelled backwards
- Part of your user ID or name
- Any common name, such as Joe
- The name of a close relative, friend or pet
- Your phone number, office number or address
- Your birthday or anniversary date
- Simple variants of names or words (even foreign words), simple patterns, famous equations or well-known values
- Your favorite sports team (NFL, NBA, MLB, etc.)
- Your license plate number, your social security number or any all-numeral password
- Names from popular culture (e.g.: Beatles, Spiderman, etc.)

Creating a Stronger Password

You should follow these guidelines when creating a password:

- Do not use your user name or any part of your real name.
- Do not use a single word in a common language. There are tools for hackers that search through electronic dictionaries, trying every word.
- Avoid characters other than those above, such as accented characters (áèôü) or characters from other alphabets (Ρωσικά, Греческий). The basic system will handle these passwords, but you may not be able to enter them correctly on web pages.
- Spell a word backwards (anomopyloplac1#).
- Insert a number (calpo7lyPomona) or punctuation (go!Broncos).
- Use weird capitalization (remember that it counts), or combine words (broNCOsrOOL!)).
- Use the first letters of each word in a phrase (“I can never remember my stupid password!” = Icnrmsp!).
- Combine things you will remember ("I like to eat broccoli and listen to Beethoven = broCColi@bEEthoven).
- Consider using a pass phrase instead of a password.

Password Managers

A password manager is software for storing all your passwords in one location that is protected and accessible with one easy-to-remember master passphrase. It is one of the best ways to keep track of each unique password or passphrase that you have created for your various online accounts—without writing them down on a piece of paper and risking that others will see them. When using a password manager, you have one master passphrase that protects all of your other passwords. This leaves you with the ease of having to remember only one.

Types of Password Managers

As Neil Randall pointed out in PC Magazine over a decade ago, “Password management utilities have proliferated with the growth of the Internet and, as Web users log on to more and more password-protected sites, have become almost indispensable tools.” There are many types of password managers. A desktop password manager is software you install on your computer’s hard drive; it stores your user name and password only on that computer. You can use a portable

password manager on your smart phone and other portable devices. Or you may choose to store your passwords on the website of a password management provider or choose multi-factor authentication, where you use a combination of ways to access a password manager on your desktop; for example, a smartcard or USB drive plus a password or, perhaps, a fingerprint. Some password managers can create new passwords for you. This eliminates the need for you to come up with dozens of unique and complex passwords and passphrases. In PC World, Paul Mitchell describes a new type of password manager that eliminates the worry about where your password manager is located: "The makers of an emerging breed of password managers are striving to provide secure online access to your passwords in the cloud and give you a synchronized, local copy of your password database on every computer and mobile device, no matter what operating systems, browsers or mobile platforms you use." If all the information is stored in the cloud, you can access it from any of your devices at any time. Moreover, in effect, the cloud provider creates a backup of your password manager file. If you do not regularly back up your desktop files, a cloud-based password manager may have important features for you to consider.

Choosing a Password Manager

Consider the type of password manager that best suits how and where you work. This is where research into the type of password manager is necessary. Ask yourself what type of passwords you will be storing and where you will most often access these sites. For example, if you have passwords only for sites that you access at home, you would not need the password manager to be stored on your mobile device. If you store a password manager on one computer and need to access your passwords on another computer, you run into problems. On the other hand, if you are using only one computer, the storage decision becomes easier. If you use a generator of one-time passwords for all your accounts, you do not have a set of passwords to store—though you may have a set of usernames.1 You need to consider whether acquiring a password manager is the best way to handle your usernames. If you have a mix of passwords you choose and one-time passwords that are generated for you, a password manager can be useful for the passwords you choose.

After you know your needs, you can investigate particular products. When researching the products, determine the security measures of each. Does the password manager use strong encryption? Does it have a lockout feature? Does it include protection from malicious activity, such as keystroke logging—and which kinds of activity? Evaluate ease of use and convenience. Look at the functionality and the interface features and think about how you will like them over the long term. Also examine support from the vendor/provider.

Look for (and evaluate) online documentation, and find out how the company interacts with its customers: email? telephone? chat? other ways? Consider cost. Is there a one-time cost or a recurring fee? Some password manager vendors provide a free trial period or charge for certain features. If the latter, which features do you consider worth the cost? Supplement your own evaluation by searching the web for articles on the top-rated password manager and analyses of the strengths and weaknesses of various products Finally keep risks in mind.

Note particularly that there is both convenience and risk associated with storing your passwords in the cloud, as noted in a previous US-CERT paper2 and there is the potential for attacks on cloud password managers. In May 2011, Brennan Slattery, reported in a PC World that the provider of an online password manager identified unusual network traffic of a size that could indicate an email address and password compromise.

All customers were asked to change their master password. Remember also that there is a risk with using your password manager in public locations, specifically if you leave the password manager open in the background on the computer. Also if you open your password manager on a public computer you may be taking the risk of key logging software being installed on the computer. This software can capture the information that you type on the keyboard, and a malicious user could steal your master password. In all cases, you must protect your master

password well; it's best to memorize it rather than write it down.

Some Final Words on Password Managers

With the growing number of necessary passwords and the amount of information that people have stored in online accounts, the Internet is an attractive place for malicious users to steal your personal information. By using complex passwords and passphrases and choosing a password manager that fits your password use habits, you can keep your information secure and protect yourself from identity thieves. Before you decide on a password manager, read reviews of the various products in order to understand how they work and what they are capable of doing. Some reviews include both strengths and weakness. Also do your own analysis by reading background information on vendors' websites. When you have chosen a password manager, get it directly from the vendor and verify that the installer is not installing a maliciously modified version by checking an MD5 hash of the installer 3 ; if a hash is not available, request one from the vendor; if the vendor cannot provide a verification method, be skeptical. Although moving to a password manager may take a little effort, in the long run it is a safe and convenient method of keeping track of your passwords and guarding your online information.

Access Control

Access control is the process by which users are identified and granted certain privileges to information,systems,or resources.Understanding the basics of access control is fundamental to understanding how to manage proper disclosure of information.

Controlling how network resources are accessed is paramount to protecting private and confidential information from unauthorized users.the type of access control machanisms available for information technology initiatives today continue to increase.most access control methodologies are based on the same underlying principles.if you understand the underlying concepts and principles,you can apply this understanding to new products and technologies and shorten the learning curve,so you can keep pace with new technology initiatives.

Access control devices properly identify people,and verify their identity through an authentication process, so that they can be held accountable for their actions.good access control systems record and timestamp all communications and transactions so that access to systems and information can be audited at later dates.

Reputable access control systems provide authentication,authorization,and administration.authentication is a process in which users are challenged for identity credentials so that it is possible to verify that they are who they say they are.once a user has been authenticated,authorization determines what resources a user is allowed to access.A user can be authenticated to a network domain,but only be authorized to access one system or file within that domain.administration refers to the ability to add,delete,and modify user accounts and user account privileges.

Objectives of Access Control

The objective of access control is to preserve and protect the confidentiality,integrity,and availability of information,systems,and resources.confidentiality refers to the assurance that only authorized individuals are able to view and access data and systems.integrity refers to protecting the data from unauthorized modification.you can have confientiality without integrity and vice versa.it is important that only the right people have access to the data,but it is also important that the data is the right data,and not data that have been modified either accidentally or on purpose.

Data availability is also the important security service.while data and resources need to be secure,they also need to be accessible and available in a timely manner.if you have to open 10 locked safes to obtain a piece of data,the data is not very available in a timely fashion.while availability may seem obvious,it is important to acknowledge that it is a goal so that security is not overdone to the point where the data is of no use to anyone.

Types of Access Control

There are four types of access control.they are as follows:

- Discretionary access control systems
- Mandatory access control systems
- Role-based access control systems
- Rule-based access control systems

Discretionary access control systems allow the owner of the information to decide who can read,write,and execute a particular file or service.when users create and modify files in their own home directories,their ability to do this is because they have been granted discretionary access control over the files that they own.on end-user laptops and desktops,discretionary access control systems are prevalent.

Mandatory access control systems do not allow the creator of the information to govern who can access it or modify data.administrators and overseeing authorities predetermine who can access and modify data,systems,and resources.madatory access control systems are commonly used in military installation,financial institutions,and in medical institutions.

Role-based access control systems allow users to access systems and information based on their role within the organization.it allows end-users access to information and resources based on their role within the organization.role-based access can be applied to groups of people or individuals.for example,you can allow everyone in a group named sysadmin access to privileged resources.

Rule-based access control systems allow users to access systems and information based on predetermined and configured rules.rules can be established that allow access to all end-users coming from a particular domain,host,network,or IP addresses.if an employee changes his role within the organization, his existing authentication credentials remain in effect and do not need to be re-configured.using rules in conjunction with roles adds greater flexibility.

Access Control Matrix

Access control matrix or access matrix is an abstract, formal security model used in computer systems that characterizes the rights of each subject with respect to every object in the system.it was first introduced by Butler W.Lampson in 1971.

According to the model,a computer systems consists of a set of objects O,that is, the set of entities that needs to be protected(e.g. processes,files,memory pages)and a set of subjects S,that consists of all active entities(e.g. users,processes). Further,there exists a set of rights R of the form r(s,o),which specifies the kind of access a subject is allowed to process with regard to an object.

Let us take an example.in this matrix example, there exists two processes,a file and some device.the first process has the ability to execute the second, read the file and write some informaion to the device,while the second process can only to the first.

	Process 1	process 2	Device	File
Process 1	Read,Write, Execute	Read	Read	Write
Process 2	Read,Execute	Read,Write, Execute		

The access control matirx can be used as a model of the static access permissions in any type of access control system.it does not model the rules by which permissions can change in any particular system,and therefore only gives an incomplete description of the system's access control security policy.

An access control matrix should be thought of only as an abstract model of permissions at a given point in time;a literal implementation of it as a two-dimensional array would have excessive memory requirements.capability-based security and access control lists are categories of concrete access control mechanisms whose static permissions can be modelled using access control matrices.although these two mechanisms have sometimes been presented as simply row-based and column-based implementations of the access control matirx,this view has been criticized as drawing a misleading equivalence between systems that do not take into account dynamic behaviour.rules can be applied to people,as well as devices.

Evidence

The **Indian Evidence Act**, originally passed in India by the Imperial Legislative Council in 1872, during the British Raj, contains a set of rules and allied issues governing admissibility of evidence in the Indian courts of law.

The enactment and adoption of the Indian Evidence Act was a path-breaking judicial measure introduced in India, which changed the entire system of concepts pertaining to admissibility of evidences in the Indian courts of law. Until then, the rules of evidences were based on the traditional legal systems of different social groups and communities of India and were different for different people depending on caste, religious faith and social position. The Indian Evidence Act introduced a standard set of law applicable to all Indians.

The law is mainly based upon the firm work by Sir James Fitzjames Stephen, who could be called the founding father of this comprehensive piece of legislation.

Law of Electronic Evidence

In the past decade or two, e-commerce has seen a huge boom. Everything from Harry Potter books to plots of land can be bought online these days. At the same time, the use of closed circuit televisions ("CCTV") to nab thieves and other miscreants has increased in shopping complexes and other public places, where instead of guards being posted at multiple places, one guard sits at a counter and keeps watch over the entire place through the CCTV recordings. Thus, both in civil as well as criminal matters, technology is assuming an increasingly important role to play.

In the case of electronic contracts, the proof of the transactions actually taking place is available only on emails, often signed with electronic signatures. In criminal proceedings, the prosecution can now use electronic evidence to prove the guilt of the accused.

However, the progression from an age of no technology to its admissibility in the court of law has come gradually over a period of time, causing paradigm shifts in many fundamental principles of the law of evidence. In this paper, the researcher seeks to show the shift that has occurred with respect to electronic evidence within two important rules of evidence – that of hearsay and that of primary evidence. The researcher looks at the earlier position of law in this regard, the reason for subsequent change, the amendments to law, and a few possible effects of such amendment.

Admissible and Relevant Evidence

The law of evidence has long been guided by the rule of "best evidence" which is considered to have two basic paradigms – avoidance of hearsay and production of primary evidence. These rules are believed to weed out infirm evidence and produce only that which cannot be reasonably be doubted. In light of the Indian Evidence Act, 1872, this can be understood as only a person who has himself perceived the fact being proved can depose with respect to it, and not someone who has received the information second hand. Similarly, where a document is to be used to prove a point, the original should be produced in court, and not a copy or photograph or any other reproduction of the same, not even statements regarding the contents by someone who has seen it. For any reproduction of a statement or document is lower on the rung of authenticity than the original, giving opportunities for fraud or fabrication.

Hearsay has been defined as "all the evidence which does not derive its value solely from

the credit given to the witness himself, but which rests also in part on the veracity and competence of some other person". Thus, if a person A chooses to depose in court that person B told him that he had seen person C stabbing person D, person A's statements with respect to the act of stabbing that occurred will be hearsay, since it is not completely out of his own knowledge, but based partly on what person B told him. However, person B's evidence will be direct evidence since he saw the act happening with his own eyes. If, on the other hand, person A's deposition were to be in respect of whether or not person B had seen the act happen, his statements would be direct evidence, since he had himself heard person B say so. Thus, it is the purpose for which a statement is being used that qualifies it as hearsay or not.

Primary evidence is the original document being itself produced for inspection by the court. A document has been defined as any matter which has expressed or described upon any substance by means of letters, marks or figures for the purpose of recording that matter. Thus, a certificate of age, an inscription on a stone plaque, a caricature or photograph, a map, are all documents of various forms. If a copy is made of such a document, it will not be primary evidence since it is not the original. Copies of the original document are considered secondary evidence. Secondary evidence is acceptable in court only under certain conditions, such as when the original is in the possession of the adversary or when the original is destroyed or lost, or when the original is of such a nature that it cannot be easily moved. So long as evidence is direct and not hearsay in nature, or is primary evidence, the court may accept it, provided that the fact being proved through such evidence proves the existence or non-existence of fact in issue to be probable in the past, presence or future, that is to say, it is a relevant fact. The Indian Evidence Act has set out a number of conditions under which a fact can be considered relevant. In other words, the condition for admissibility of a piece of evidence is that it should prove a relevant fact.

New Forms of Evidence

While there can be no limit to the forms in which evidence exists, they were so far broadly classified into oral and documentary. Documentary evidence was usually such as could be put down on paper – certificates, executed deeds, photographs, maps, caricatures, etc. Slowly, as records began to be made on objects such as cassettes and gramophone discs, those began being entertained as documents too.Recently, in February 2010, the city of Pune was endangered by a terrorist attack in a much-frequented bakery. The German Bakery blast accused were finally identified by the police on the basis of a CCTV recording. The question, therefore, arises as to whether such a recording, which is neither on paper nor on a camera negative nor on a magnetic tape, in fact, not available in any tangible form at all, can be introduced in court as evidence. The only proof available will be that recorded in the computer system controlling the CCTV unit.

This example brings into focus the very recent phenomenon of the increasing use of computers in everyday life. With the facility of writing letters over the internet being widely available now, more and more contracts are being entered into online. Thus, people can now order products online, and the sellers will ship the consignment across, the payment being made through e-banking. A director and actor may enter into a contract regarding a film through emails. The Chief Executive Officer of a company may confirm the job application of an interviewee over emails. All forms of communication and contract formation which earlier took place face-to-face or through letters can now happen over the internet. Thus, if any of the parties to the contract were to sue each other for breach of contract, the only adducible evidence would be the text of the emails.

On the other side of the spectrum, technology is also being used to plan out criminal activities. The gruesome case of the terror attacks in Mumbai in 2008 brought to light how well terrorists are versed with technology these days, and how they use them to their benefit. The terrorist controllers had purchased Voice Over Internet Protocol (VOIP) connections, making payments through Western Union Money Transfer, so as to stay in touch with the attackers and

give them instructions from Pakistan. The details of the internet transactions were provided as evidence by the prosecution in the Trial Court.

Classification of Electronic Evidence

Under the Indian Evidence Act, any substance on which matter has been expressed or described can be considered a document, provided that the purpose of such expression or description is to record the matter. Electronic records have been defined in the Information Technology Act, 2000 as any data, record or data generated, any image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche. An electronic record can be safely included under such a definition because matter is recorded on the computer as bits and bytes, which are the digital equivalent of figures or marks. Computer records were widely considered to be hearsay statements since any information retrieved from a computer would consist of input provided by a human being. Thus, be it a word document containing statements written by one party, or an image of a missing person generated by the computer based on inputs given to it, all such records will be hearsay.

An electronic document would either involve documents stored in a digital form, or a print out of the same. What is recorded digitally is a strictu sensu document, but cannot be perceived by a person not using the computer system into which that information was initially fed. Thus, if music composer A mixed certain tunes on his computer, and another composer, B, wanted to sue him for copyright violation, B would not have access to the digital records on A's computer. Even though such a document can be imprinted onto a magnetic base, such as a compact disc (CD), it would still require access to A's computer. A document containing a print out of computer records, though a document lato sensu, can be perceived by anybody. Such print outs of documents would amount to secondary evidence going strictly by the provisions of the Indian Evidence Act.

Electronic documents strictu sensu were admitted as real evidence, that is, material evidence, but such evidence requires certification with respect to the reliability of the machine for admission. In R v. Wood, where the prosecution sought to rely on a comparison of a computer analysis of certain processed metals to that of metals found in the defendant's possession, the Court held that since the computer had been used as a calculator, the analysis could be admitted as real evidence. Being both hearsay as well as secondary evidence, there was much hesitation regarding the admissibility of electronic records as evidence.

Shifting Paradigms – Admitting Electronic Records as Evidence

In the United Kingdom, hearsay computer records were made admissible in 1995 through an amendment to their Civil Evidence Act, 1968 because of the lack of objections raised by parties to such evidence over a period of time, indicating its acceptance amongst the general public.

With respect to criminal cases, the position of law following the decision in R v. Wood changed with the decision in Castle v. Cross wherein the prosecution sought to rely on a print out from a computerised breath-testing device. The Court held that the print-out was admissible evidence. The position of law was clarified in the leading case of R v. Shephard. In this case, records from till rolls linked to a central computer in a shop were produced to prove that items in possession of the accused had not been billed and had thus been stolen by the accused. The issue was whether a document produced by a computer can be produced as evidence. The Court held that so long as it could be shown that the computer was functioning properly and was not misused, a computer record can be admitted as evidence. In India, the change in attitude came with the amendment to the Indian Evidence Act in 2000. Sections 65A and 65B were introduced into the chapter relating to documentary evidence. Section 65A provides that contents of electronic records may be admitted as evidence if the criteria provided in Section 65B is complied with. Section 65B provides that shall be considered documents, thereby making it primary evidence, if the computer which produced the record had been regularly in use, the

information fed into the computer was part of the regular use of the computer and the computer had been operating properly. It further provides that all computer output shall be considered as being produced by the computer itself, whether it was produced directly or indirectly, whether with human intervention or without. This provision does away with the concept of computer evidence being hearsay.

Thus, with the amendments introduced into the statute, electronic evidence in India is no longer either secondary or hearsay evidence, but falls within the best evidence rule.

Effects of Considering Electronic Evidence as Primary and Direct

Blurring the Difference between Primary and Secondary Evidence

By bringing all forms of computer evidence into the fold of primary evidence, the statute has effectually blurred the difference between primary and secondary forms f evidence. While the difference is still expected to apply with respect to other forms of documents, an exception has been created with respect to computers. This, however, is essential, given the complicated nature of computer evidence in terms of not being easily producible in tangible form. Thus, while it may make for a good argument to say that if the word document is the original then a print out of the same should be treated as secondary evidence, it should be considered that producing a word document in court without the aid of print outs or CDs is not just difficult, but quite impossible.

Making Criminal Prosecution Easier

In light of the recent spate of terrorism in the world, involving terrorists using highly sophisticated technology to carry out attacks, it is of great help to the prosecution to be able to produce electronic evidence as direct and primary evidence in court, as they prove the guilt of he accused much better than having to look for traditional forms of evidence to substitute the electronic records, which may not even exist. As we saw in the Ajmal Kasab case, terrorists these days plan all their activities either face-to-face, or through software. Being able to produce transcripts of internet transactions helped the prosecution case a great deal in proving the guilt of the accused.

Similarly, in the case of State (NCT of Delhi) v. Navjot Sandhu @ Afsan Guru, the links between the slain terrorists and the masterminds of the attack were established only through phone call transcripts obtained from the mobile service providers.

Risk of Manipulation

While allowing all forms of computer output to be admissible as primary evidence, the statute has overlooked the risk of manipulation. Tampering with electronic evidence is not very difficult and miscreants may find it easy to change records which are to be submitted in court. However, technology itself has solutions for such problems. Computer forensics has developed enough to find ways of cross checking whether an electronic record has been tampered with, when and in what manner.

Opening Potential Floodgates

Computers are the most widely used gadget today. A lot of other gadgets involve computer chips in their functioning. Thus, the scope of Section 65A and 65B is indeed very large. Going strictly by the word of the law, any device involving a computer chip should be adducible in court as evidence. However, practical considerations as well as ethics have to be borne in mind before letting the ambit of these Sections flow that far. For instance, the Supreme Court has declared test results of narco-analysis to be inadmissible evidence since they violate Article 20(3) of the Constitution. It is submitted that every new form of computer technology that is sought to be used in the process of production of evidence should be subjected to such tests of

Constitutionality and legality before permitting their usage.

It has thus been seen that with the increasing impact of technology in everyday life, the production of electronic evidence has become a necessity in most cases to establish the guilt of the accused or the liability of the defendant. The shift in the judicial mindset has occurred mostly in the past twenty years and most legal systems across the world have amended their laws to accommodate such change.

In India, all electronic records are now considered to be documents, thus making them primary evidence. At the same time, a blanket rule against hearsay has been created in respect of computer output. These two changes in the stance of the law have created paradigm shifts in the admissibility and relevancy of electronic evidence, albeit certain precautions still being necessary. However, technology has itself provided answers to problems raised by it, and computer forensics ensure that manipulations in electronic evidence show up clearly in the record. Human beings now only need to ensure that electronic evidence being admitted is relevant to the fact in issue and is in accordance with the Constitution and other laws of the land.

"CYBER SECURITY IS A SHARED RESPONSIBILITY, AND IT BOILS DOWN TO THIS: IN CYBER SECURITY, THE MORE SYSTEMS WE SECURE, THE MORE SECURE WE ALL ARE"

- JEH JOHNSON