INFORMATION AND CYBER SECURITY

UNIT-1

ESSENTIAL TERMINOLOGIES:

- **Computer Security**-generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security**-measures to protect data during their transmission. This area covers the use of cryptographic algorithms in network protocols and network applications.

  Terms Information security and Cyber security are often used interchangeable.

- **Information Security**: It is all about protecting information from unauthorized users, access, and data modification or removal in order to provide confidentiality, integrity, and availability.
- **Cyber Security**: It is the practice of protecting the data from outside the resource on the internet.
- **Security Principles**

There are three security principles.

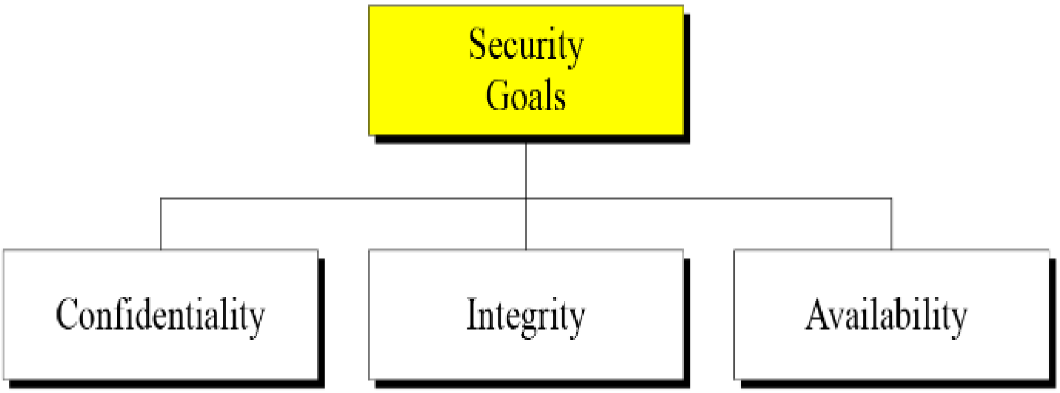
❑ Confidentiality

❑ Integrity

❑ Availability

Confidentiality

- Confidentiality is probably the most common aspect of information security. We need to protect our confidential information. An organization needs to guard against those malicious actions that endanger the confidentiality of its information.
- Example: Industrial Confidential data, Bank



Integrity

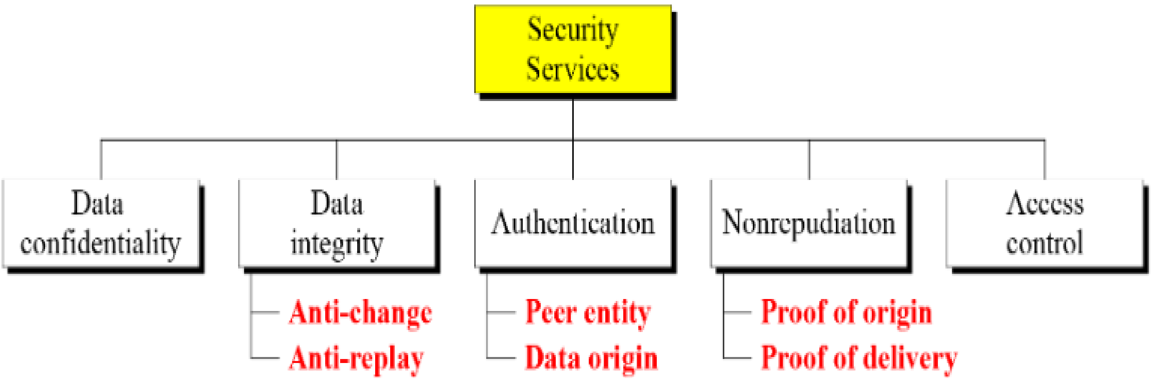
- Information needs to be changed constantly. Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.
- Example: Bank data should be automatically updated after any transaction.

Availability

- The information created and stored by an organization needs to be available to authorized entities. Information needs to be constantly changed, which means it must be accessible to authorized entities.
- Example: Accessing of information anywhere at any time.

SECURITY SERVICES

- ITU-T (**International Telecommunication Union – Telecommunication standards**)provides some security services and some mechanisms to implement those services.
- Security services and mechanisms are closely related because a mechanism or combination of mechanisms are used to provide a service.



- **Confidentiality:** information is not made available to unauthorized individual
- **Integrity:** assurance that the message is unaltered
- **Authentication:** assures recipient that the **message is from the source** that it **claims to** be from.

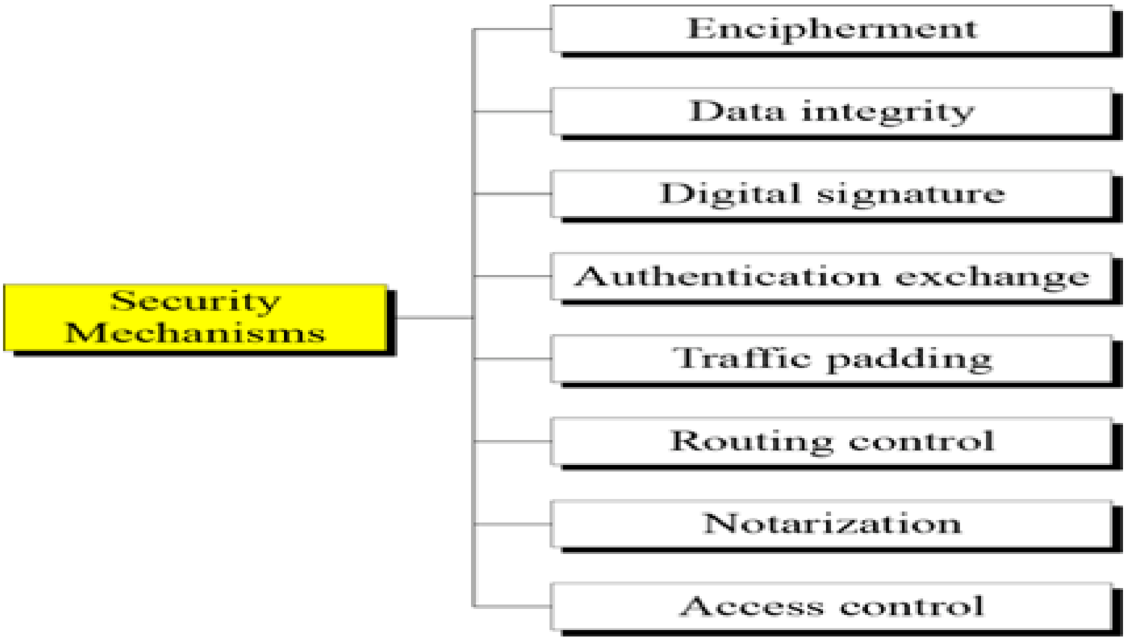
  Peer entity authentication: Provides for the corroboration of the identity of a peer entity in an association. Two entities are considered peers if they implement to same protocol in different systems; e.g., two TCP modules in two communicating systems.

  Data origin authentication: Provides for the corroboration of the source of a data unit. It does not provide protection against the duplication or modification of data units

- **Non-Repudiation:** protection against denial of sending or receiving in the communication
- **Access Control:** controls who can have **access to resource** under what **condition**
- **Availability:** available to authorized entities for 24/7.

SECURITY MECHANISMS

- The security mechanisms defined in X.800. As can be seen the mechanisms are divided into those that are implemented in a specific protocol layer and those that are not specific to any particular protocol layer or security service.



Encipherment

- The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

Data Integrity

- A variety of mechanisms used to assure the integrity of a data unit or stream of data units

Authentication Exchange

- A mechanism intended to ensure the identity of an entity by means of information exchange.

Digital Signatures

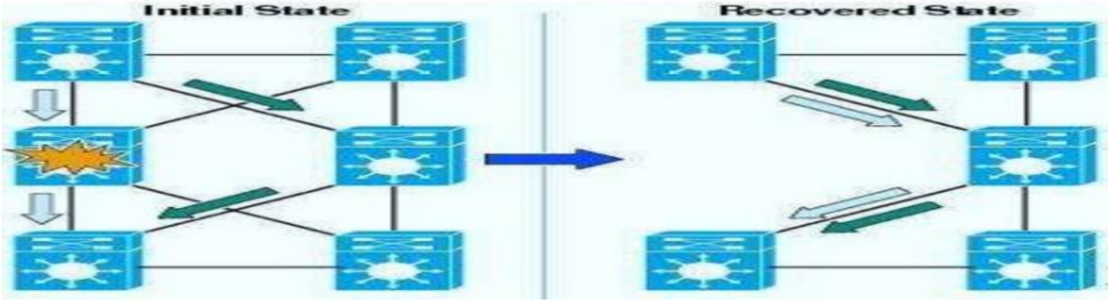
A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document.

Traffic Padding

- The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

Routing Control

- Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.



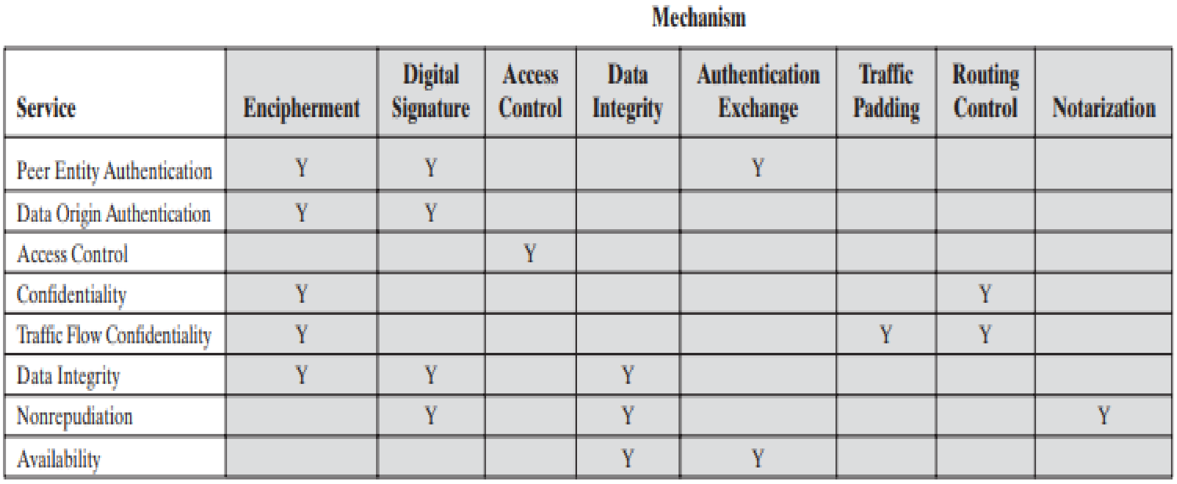
Notarization

- The use of a trusted third party to assure certain properties of a data exchange.

Access Control

- A variety of mechanisms that enforce access rights to resources. Ex: pwd &pins

Relationship Between Security Services and Mechanisms

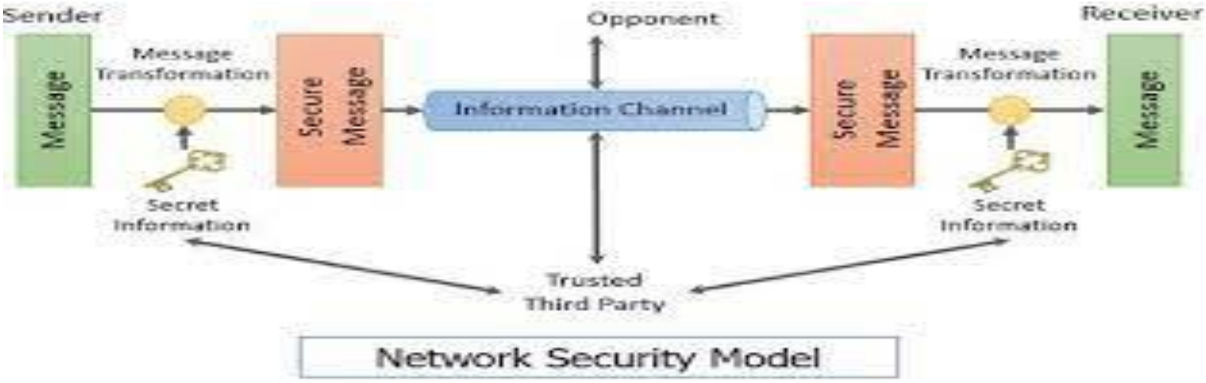


Mechanism

Service	Encipherment	Digital Signature	Access Control	Data Integrity	Authentication Exchange	Traffic Padding	Routing Control	Notarization
Peer Entity Authentication	Y	Y			Y			
Data Origin Authentication	Y	Y						
Access Control			Y					
Confidentiality	Y						Y	
Traffic Flow Confidentiality	Y					Y	Y	
Data Integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

NETWORK SECURITY MODEL

- Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on.
- All the techniques for providing security have two components:



- A security-related transformation on the information to be sent.
- Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.
- Some secret information shared by the two principals and, it is hoped, unknown to the opponent.
- An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.
- A trusted third party may be needed to achieve secure transmission.
- For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent.
- This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

NIA – NATIONAL INVESTIGATION AGENCY

- National Investigation Agency (NIA) is functioning as the Central Counter Terrorism Law Enforcement Agency in the country.
- Information is given about the NIA's mission, objectives, banned organisations, NIA special courts, nodal officers and branch offices etc.
- A list of wanted by NIA is also provided. Ex: Al-Qaida
- Helpline numbers and contact details of officers are available.
- Users can also access the case details under the Agency.

RISKS

- The term “information security risk” refers to the damage that attacks against IT systems can cause.
- IT risk encompasses a wide range of potential events, including data breaches, regulatory enforcement actions, financial costs, reputational damage, and more.
- Although “risk” is often conflated with “threat,” the two are subtly different.
- “Risk” is a more conceptual term: something that may or may not happen.
- A “threat” is a specific, actual danger.

Risk Assessments

- Identify –Identifying security risk
- Analyse -- examine each risk and determine both its likelihood of occurring and the potential impact.
- Prevent--to develop controls and procedures to either minimize the damage or prevent it altogether
- Document--Clear documentation of your policies and risk mitigation efforts will serve you well long term.
- Monitor and Reassess -- monitor the success of your security efforts, reassess your risks periodically (usually once a year), and adjust your policies, procedures, and controls as necessary.

Risk Responses

- **Accept** --This response understands that a certain amount of risk is always present. Also known as risk retention, risk acceptance is the decision that the potential gain for a given scenario outweighs the chance of loss.

- **Share** --Another common strategy is to share risk with an outside contractor or partner. An example of risk sharing in IT risk management would be using a cloud storage service like AWS or Microsoft Azure.
- **Transfer** -- Risk transfer is when you move the responsibility for the risk onto an outside party. This is usually done by purchasing insurance for the issue in question.
- **Avoid**--Risk avoidance is generally the safest of these strategies.

BREACHES

- A security breach is any incident that results in unauthorized access to computer data, applications, networks or devices. It results in information being accessed without authorization. Typically, it occurs when an intruder is able to bypass security mechanisms.
- Technically, there's a distinction between a security breach and a data breach. A security breach is effectively a break-in, whereas a data breach is defined as the cybercriminal getting away with information.

Examples of a security breach

- Yahoo --3 billion user accounts were compromised in 2013 after a phishing attempt gave hackers access to the network.
- eBay saw a major breach in 2014. Though PayPal users' credit card information was not at risk, many customers' passwords were compromised.
- Facebook saw internal software flaws lead to the loss of 29 million users' personal data in 2018.
- Marriott Hotels announced a security and data breach affecting up to 500 million customers' records in 2018.

Types of security breaches

There are a number of types of security breaches depending on how access has been gained to the system:

- An exploit attacks a system vulnerability, such as an out of date operating system. Legacy systems which haven't been updated, for instance, in businesses where outdated and versions of Microsoft Windows that are no longer supported are being used, are particularly vulnerable to exploits.
- Weak passwords can be cracked or guessed. Even now, some people are still using the password 'password', and 'pa$$word' is not much more secure.
- Malware attacks, such as phishing emails can be used to gain entry. It only takes one employee to click on a link in a phishing email to allow malicious software to start spreading throughout the network.
- Drive-by downloads use viruses or malware delivered through a compromised or spoofed website.

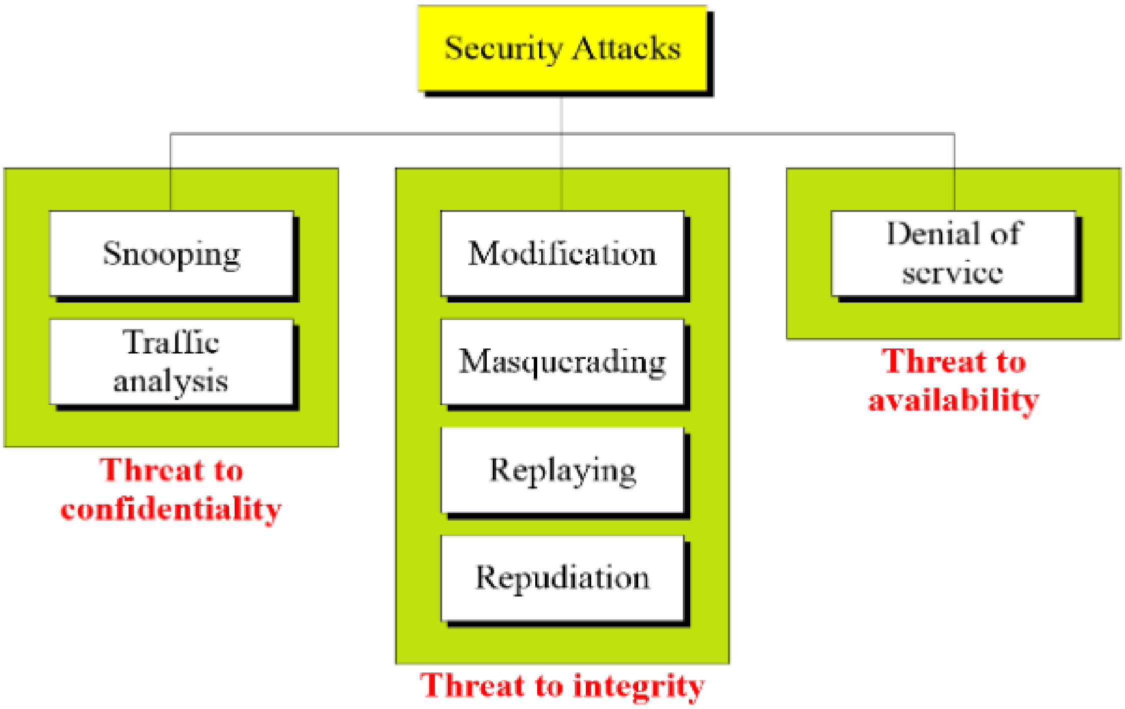
- Social engineering can also be used to gain access. For instance, an intruder phones an employee claiming to be from the company's IT helpdesk and asks for the password in order to 'fix' the computer.

THREATS

- Type of unwanted access is the placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs, such as editors and compilers.
- Programs can present two kinds of threats:
- Information access threats: Intercept or modify data on behalf of users who should not have access to that data.
- Service threats: Exploit service flaws in computers to inhibit use by legitimate users

ATTACKS

- The three goals of security confidentiality, integrity, and availability can be threatened by security attacks.
- Attacks Threatening Confidentiality
- Attacks Threatening Integrity
- Attacks Threatening Availability



Attacks Threatening Confidentiality

Snooping refers to unauthorized access to or interception of data.

Traffic analysis refers to obtaining some other type of information by monitoring online traffic.

Attacks Threatening Integrity

Modification means that the attacker intercepts the message and changes it.

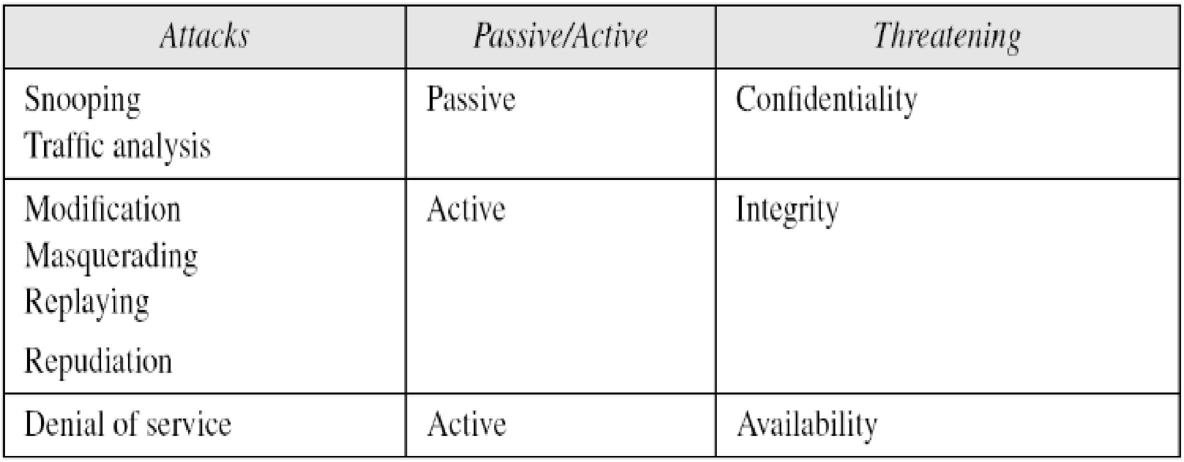
Masquerading or spoofing happens when the attacker impersonates somebody else.

Replaying means the attacker obtains a copy of a message sent by a user and later tries to replay it.

Repudiation means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

Attacks Threatening Availability

Denial of service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system.



Attacks	*Passive/Active*	*Threatening*
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

EXPLOITS

- An exploit is a code that takes advantage of a software vulnerability or security flaw.
- exploits allow an intruder to remotely access a network and gain elevated privileges, or move deeper into the network.
- In some cases, an exploit can be used as part of a multi-component attack. Instead of using a malicious file, the exploit may instead drop another malware, which can include backdoor Trojans and spyware that can steal user information from the infected systems.

Zero-Day Exploits and Exploit Kits

- an exploit is referred to as a zero-day exploit when it is used to attack a vulnerability that has been identified but not yet patched, also known as a zero-day vulnerability.
- Exploits are often incorporated into malware, allowing them to propagate and run intricate routines on vulnerable computers
- Exploit kits are popular in the cybercriminal underground because they provide management consoles, an array of exploits that target different applications, and several add-on functions that make it easier to launch an attack.

Mitigating Exploits

- Virtual patching is one of the most recommended mitigation solutions for enterprises. Virtual patching works on the premise that exploits take a definable path to and from an application in order to use a software flaw.

INFORMATION GATHERING

- Gathering information is the first step where a hacker tries to get information about the target.
- Information Gathering is the act of gathering different kinds of information against the targeted victim or system.
- It is the first step or the beginning stage of Ethical Hacking, where the penetration testers or hackers (both black hat or white hat) performed this stage; this is a necessary and crucial step to be performed.
- The more the information gathered about the target, the more the probability to obtain relevant results.
- Information gathering is not just a phase of security testing; it is an art that every penetration-tester (pen-tester) and hacker should master for a better experience in penetration testing.
- There are various tools, techniques, and websites, including public sources such as Whois, nslookup that can help hackers gather information.
- This step is necessary because you may need any information (such as his pet name, best friend's name, age, or phone number to perform password guessing attack or other kinds of attacks) while performing attacks on any target.
- Information gathering can be classified into three categories
    - Footprinting: Footprinting is the technique to collect as much information as possible about the targeted network/victim/system. It helps hackers in various ways to intrude on an organization's system. Footprinting can be active as well as passive.
    - Scanning:
    - Enumeration

INCIDENT RESPONSE TEAM

- An incident response team is a group of IT professionals in charge of preparing for and reacting to any type of organizational emergency.
- Responsibilities of an incident response team include developing a proactive incident response plan, testing for and resolving system vulnerabilities, maintaining strong security best practices and providing support for all incident handling measures.

- Incident response team members typically cover various technical skills, backgrounds and roles to be prepared for a wide range of unforeseen security incidents.

In incident response, types of emergencies are usually categorized in two ways:

1. Public incidents. These incidents affect an entire community. This could include natural disasters, terrorist attacks and widespread epidemics.
2. Corporate/organizational incidents. These incidents are typically organization-specific and happen on a smaller scale. This could include data breaches, cybersecurity attacks and physical location threats.

   Incident response teams are trained to be prepared for both types

   Examples of incident response teams

- Computer Security Incident Response Team (CSIRT). This is a team of professionals responsible for preventing and responding to security incidents.
- Computer Emergency Response Team (CERT). This is a team of professionals in charge of handling cyberthreats and vulnerabilities within an organization.
- Security Operations Center (SOC). This is a type of command center facility that is dedicated to monitoring, analyzing and protecting an organization from cyber attacks.

Incident response team functions and responsibilities::

Generally speaking, the core functions of an incident response team include leadership, investigation, communications, documentation and legal representation.

- Leadership. Coordinates the overall direction and strategy of response activities and ensures the team stays focused on minimizing damage, recovering quickly and operating efficiently.
- Investigation. Coordinates efforts to determine an incident's root cause. It's important to gather as much relevant information as possible. Specifically, information that can provide value to correct the acute issue as well as prevent future issues.
- Communications. Manages relevant internal and external communications necessary for the incident response. Communications may be required across an organization's teams and departments, or with external stakeholders.
- Documentation. Keeps records of incident response measures and activities.
- Legal representation. Ensures that the incident response activities taken line up with laws and regulations to protect the organization.

REPORTING CRIME

Examine the reporting of crime

1. Why do we need people to report crime?

2. Why don’t people report crime?

3. How can we encourage people to report crime?

1. Why do we need people to report crime?

Laws reflect the values of society – there is an expectation that members of society will hold others to account for breaching those laws

Police don’t observe most crimes being committed; they are reliant on people to report crimes Police are responsible for enforcing laws – members of society must bring crimes to their attention

1. How can we encourage people to report crime?

1. Make it easier to report crimes Currently 000, Crime Stoppers, local police station (phone or physical presence) Maybe an app? Text services ;) 2. Educate people (TV, schools, social media, posters…) What constitutes a crime? All crimes matter How to report crime Crime/safety is everyone’s responsibility.

OPERATING SYSTEM ATTACKS

- Operating Systems attacks, “attackers look for vulnerabilities in OS such that they can exploit through vulnerabilities and gain access to the target system or network”.
- The vulnerabilities in the OS can be open ports and services as most of the operating systems install these services and ports by default. These are the most common vulnerabilities found by attackers to gain access to an operating system.
- Some of the OS vulnerabilities list
  - Buffer Overflow Vulnerability
  - Bugs in the operating system
  - Unpatched Operating System
- Some of the attacks performed by OS Level
  - Exploiting specific network protocol implementation
  - Attacking built-in Authentication System
  - Breaking file-system Security

- Cracking Passwords and Encryption Mechanism

APPLICATION ATTACKS

- Examples of Application level Attacks
    - Buffer Overflow : A buffer overflow attack typically involves violating programming languages and overwriting the bounds of the buffers they exist on.
    - Session hijacking :: an attacker hijacks a session between a trusted client and network server.
    - Phinsing :Phishing is a social engineering attack entailing fraudulent communications appearing to come from a trusted source. Phishing attack is that the practice of sending emails that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something.
    - Denial-of-service : It prevents normal use of communication facilities. This attack may have a specific target.
    - Man-in-the-middle::A MITM (man-in-the-middle) attack is one where the attacker intercepts and relays messages between two parties who believe they are interacting with one another.
    - SQL injection:: SQL injection has become a common issue with database-driven websites. a/c username and password ‘1’ = ‘1’

REVERSE ENGINEERING

- Reverse-engineering is the act of dismantling an object to see how it works.
- It is done primarily to analyze and gain knowledge about the way something works but often is used to duplicate or enhance the object.
- Many things can be reverse-engineered, including software, physical machines, military technology and even biological functions related to how genes work.
- The practice of reverse-engineering as applied to computer hardware and software is taken from older industries.
- Software reverse-engineering focuses on a program's machine code -- the string of 0s and 1s that are sent to the logic processor.
- Program language statements are used to turn the machine code back into the original source code.

Purpose of reverse-engineering

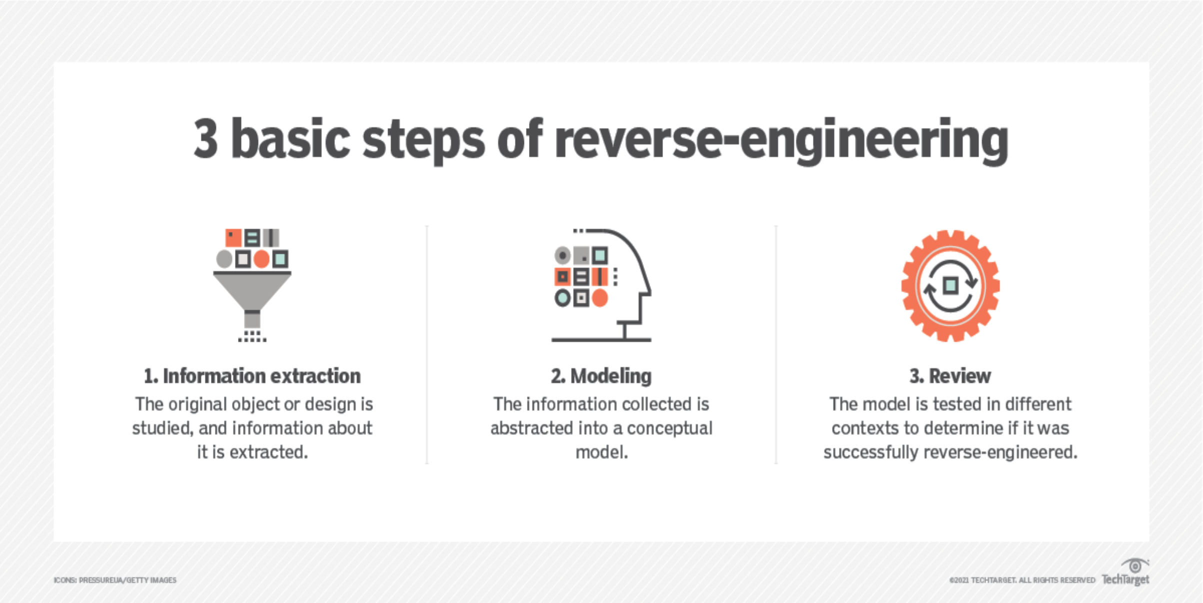
- The purpose of reverse-engineering is to find out how an object or system works. There are a variety of reasons to do this. Reverse-engineering can be used to learn how something works and to recreate the object or to create a similar object with added enhancements.
- Goal:: reverse-engineering software or hardware is to find a way to create a similar product more inexpensively or because the original product is no longer available.

- Reverse-engineering in information technology is also used to address compatibility issues and make the hardware or software work with other hardware, software or operating systems that it wasn't originally compatible with.

How does the reverse-engineering process work?

The reverse-engineering process is specific to the object on which its being performed. However, no matter the context, there are three general steps common to all reverse-engineering efforts. They include:

- Information extraction. The object being reverse-engineered is studied, information about its design is extracted and that information is examined to determine how the pieces fit together. In software reverse-engineering, this might require gathering source code and related design documents for study. It may also involve the use of tools, such as a disassembler to break apart the program into its constituent parts.
- Modeling. The collected information is abstracted into a conceptual model, with each piece of the model explaining its function in the overall structure. The purpose of this step is to take information specific to the original and abstract it into a general model that can be used to guide the design of new objects or systems. In software reverse-engineering this might take the form of a data flow diagram or a structure chart.
- Review. This involves reviewing the model and testing it in various scenarios to ensure it is a realistic abstraction of the original object or system. In software engineering this might take the form of software testing. Once it is tested, the model can be implemented to reengineer the original object.



3 basic steps of reverse-engineering

1. Information extraction
The original object or design is studied, and information about it is extracted.

2. Modeling
The information collected is abstracted into a conceptual model.

3. Review
The model is tested in different contexts to determine if it was successfully reverse-engineered.

ICONS: PRESSUREUA/GETTY IMAGES

©2021 TECHTARGET. ALL RIGHTS RESERVED TechTarget

CRACKING TECHNIQUES

Password cracking is the process of using an application program to identify an unknown or forgotten password to a computer or network resource. It can also be used to help a threat actor obtain unauthorized access to resources.

Password cracking is a process of recovering passwords from data that have been stored in or transmitted by a computer system. Examples of guessable passwords include:

1. Blank (none);
2. the words like "password," "passcode" and "admin";
3. series of letters from the "QWERTY" keyboard, for example, qwerty, asdf or qwertyuiop;
4. user's name or login name;
5. name of user's friend/relative/pet;
6. user's birthplace or date of birth, or a relative's or a friend's;
7. user's vehicle number, office number, residence number or mobile number;
8. name of a celebrity who is considered to be an idol (e.g., actors, actress, spiritual gurus) by the user;
9. simple modification of one of the preceding, such as suffixing a digit, particularly 1, or reversing the order of letters.

- Password cracking attacks can be classified under three categories as follows:
- 1. Online attacks;
- 2. offline attacks;
- 3. non-electronic attacks (e.g., social engineering, shoulder surfing and dumpster diving).

Online Attacks

- The most popular online attack is man-in-the middle (MITM) attack, also termed as "bucket-brigade attack" or sometimes "Janus attack."
- It is a form of active eavesdropping in which the attacker establishes a connection between a victim and the server to which a victim is connected.

Offline Attacks

- Offline attacks usually require physical access to the computer and copying the password file from the system onto removable media.
- Strong, Weak and Random Passwords
- A weak password is one, which could be easily guessed, short, common and a system default password that could be easily found by executing a brute force attack and by using a subset of all possible passwords.

- A strong password is long enough, random or otherwise difficult to guess – producible only by
- the user who chooses it.
- Random Passwords
- Password is stronger if it includes a mix of upper and lower case letters, numbers and other symbols, when allowed, for the same number of characters.

FINANCIAL FRAUDS

Credit card processing is a relatively new service that will allow a person to process credit cards electronically, virtually anywhere.

- it allows businesses to process transactions from mobile locations quickly, efficiently and professionally.
- It is most often used by businesses that operate mainly in a mobile environment.
- Some upscale restaurants are using wireless processing equipment for the security of their credit card paying customers.
- Figure 1 shows the basic flow of transactions involved in purchases done using credit cards.

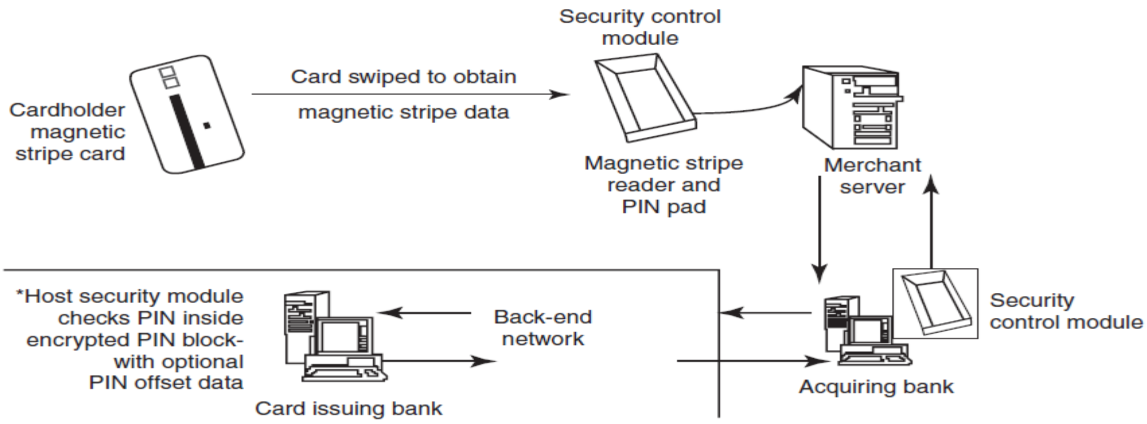

Security control module
Cardholder magnetic stripe card
Card swiped to obtain magnetic stripe data
Magnetic stripe reader and PIN pad
Merchant server
*Host security module checks PIN inside encrypted PIN block- with optional PIN offset data
Back-end network
Card issuing bank
Security control module
Acquiring bank

Figure 1 Online environment for credit card transactions.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

Do's

1. Put your Signature on the card immediately upon its receipt.

2. Make the photocopy of both sides of your card and preserve it at a safe place to remember the card number, expiration date in case of loss of card.

3. Change the default personal identification number (PIN) received from the bank before doing any transaction.

4. Always carry details about contact numbers of your bank in case of loss of your card.

5. Carry your cards in a separate pouch/card holder than your wallet.

6. Keep an eye on your card during your transaction, and ensure to get it back immediately.

7. Preserve all the receipts to compare with credit card invoice.

8. Reconcile your monthly invoice /Statement with your receipts.

9. Report immediately any discrepancy observed in the monthly invoice/statement.

10. Destroy all the receipts after reconciling it with the monthly invoice/statement.

11. Inform your bank in advance, about any change in your contact details such as home address, cell phone number and E-mail address.

12. Ensure the legitimacy of the website before providing any of your card details.

13. Report the loss of the card immediately in your bank and at the police station if necessary.

Dont's :

1. Store your card number and your PINs in your cell.

2. Leave your cards to anyone.

3. Leave cards or transaction receipts lying around.

4. Sign a blank receipt (if the transaction details are not legible, ask for another receipt to ensure the amount instead of trusting the seller).

5. Write your card number/PIN on a postcard or the outside of an envelope.

6. Give out immediately your account number over the phone (unless you are calling to a company/to your bank).

7. Destroy credit card receipts by simply dropping into garbage box/dustbin.

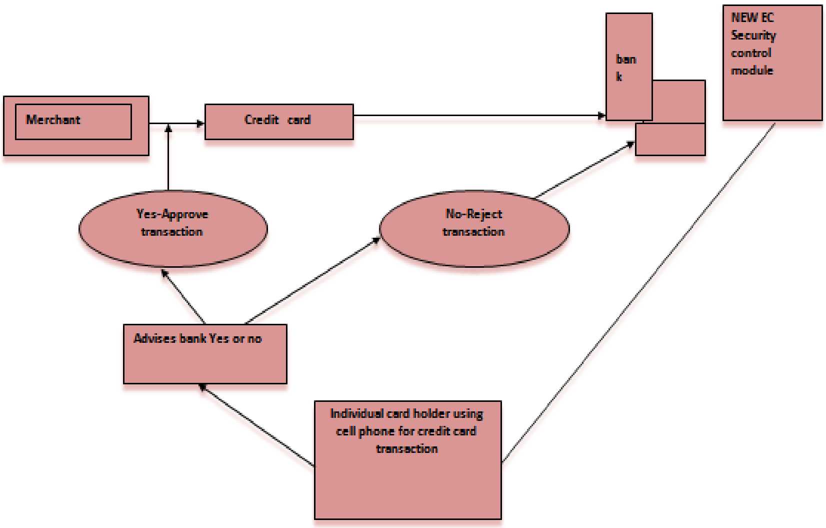
An Australian company "Alacrity" called closed-loop environment for wireless **(CLEW).**

Flow of events with CLEW is as follows:

1. Merchant sends a transaction to bank.
2. The bank transmits the request to the authorized cardholder

[not short message service(SMS)];

1. The card holder approves or rejects (password protected);
2. The bank/merchant is notified;
3. The credit card transaction is completed.



Types and Techniques of Credit Card Frauds:

1.Traditional Techniques

Applications:

1.ID Theft :

Where an individual pretends to be someone else.

2. Financial Fraud:

Where an individual gives false information about his

or her financial status to acquire credit

2.Modern Techniques:

- ➢ Skimming to commit fraud - the information held on either the magnetic strip on the back of the credit card or the data stored on the smart chip are copied from one card to another.
- ➢ Site cloning and false merchant sites on the Internet - designed to get people to hand over their credit card details.

1. Triangulation

2.Credit card Generators

UNIT-2

Cyber Offences

Introduction:

- Understand different types of cyber attacks
- Overview of the steps in planning cybercrime
- Understand tools used for gathering information about the target. etc
- Hackers:
  - Very talented, smart people who understand computers better than others
  - Hackers enjoy to learn and experimenting with the computers
- Crackers:
  - "Breaks into computers"
- Phreakers:
  - Breaks into phone lines.

Categories of Vulnerabilities

- Inadequate border protection
- Remote access servers (RAS) with weak access controls.
- Application servers with well-known exploits
- Misconfigured systems and systems with default configuration.

How Criminals plan the attack?

- Criminals use many methods and tools to identify vulnerabilities of their target.
- Criminals plan attacks were categorised into
  - Active
  - Passive
  - Inside
  - Outside
- **Active Attacks:**
  - Def: To alter the system
  - Affects: Availability, Integrity and authenticity of data.
- **Passive Attacks:**
  - Def: To gain information about the target.
  - Affects: Confidentiality

- **Inside Attack :**
  - Def: Attempted within the security perimeter of an organisation.
  - Affects: Access more resources than expected.
- **Outside attack:**
  - Def: Attempted by a source outside the security perimeter (insider/outsider) who is indirectly associated with the organisation.
  - Sources: Either from internet or a remote access connection.

Phases to plan cyber crime

- Information gathering. (passive attack)
- Reconnaissance : To gain information about an enemy .
- Starts with Foot printing.
- Scanning and scrutinizing the information.
- For the validity of the information.
- To identify the existing vulnerabilities.
- Launching an attack
- Gaining and maintaining the system access.

Passive Attack

- Information gathering about a target without their knowledge.
  - Ex: Watching a building to identify employees entering time
- It is done using internet search or googling to gain individual or company information.
- Google or Yahoo search to locate information about employees.
  - Tools:
  - *GOOGLE EARTH: It is a virtual map of globe and* geographic information program. It maps the earth by the superimposition of images obtained from satellite imagery and provides aerial photography of the globe

Ex: (www.earth.google.com).

- *INTERNET ARCHIVE: The internet archive is an internet* library with the purpose of offering permanent access for researchers, historians and scholars to historical collections that exist in digital format (Ramot *et al.,* 2003). It includes texts, Audio moving images and software as well as archived web pages in our collections.

Ex: (www.archiv.org).

- *PEOPLE SEARCH: People search provides details* about personal information, date of birth, residential address, contact number etc. Ex: (www.whitepagesinc.com).

- *DOMAIN NAME CONFIRMATION: To perform searches* for domain names using multiple keywords, this helps to find every registered domain name in "com", "netr", "org", "edu" (www.namedroppers.com).
- *WHOIS: This is a domain registration lookup tool.* This utility is used for communicating with WHOIS servers located around the world to obtain domain registration information. WHOIS supports IP address queries and automatically selects the appropriate server for IP address. This tool will lookup information on a domain IP address or a domain registration server or you can use the default option which will select a server for you (www.whois.net).
- *NSLOOKUP: The name nslookup means "name server* lookup", the tool is used on windows and Unix to query details, including up addresses of a particular computer and other technical details such as mail exchanger records for a domain and name severs of a domain (www.nslookup.downloadsoftware4free.com).
- *eMailTrackerPro: eMailTrackerPro analyzes the E-mail* header and provides the IP address of the system that send the mail (www.emailtrackerpro.com).
- *HTTrack: This tool acts like an offline browser. It can* mirror the entire website to a desktop. One can analyze the entire websites by being offline (www.httrack.com).

Active Attacks

- ARPING: This is a network tool that
  - Broadcasts arp packets and receive replies similar to "ping".
  - It is good for mapping a local network and finding used IP space
  - It broadcasts, who has an arp packet on the network and prints answers.
  - It is very useful when trying to pick an unused IP for a net to which routing does not exist as yet
- Bing: This tool is used
  - for pinging the bandwidth.
  - It is one of the point-to-point bandwidth measurement tool
  - It can calculate the blank throughput between any couple of networks. (htttp:ai3.asti.dost.gov.ph/sat/bing.html).
- It is also called "Rattling the doorknobs" or "Active reconnaissance"
- It can provide confirmation to an attacker about security measures in place .

Tools:

- **Dsniff** : This is network auditing tool to capture username, password and authentication information on a local subnet.
- **DNStracer**: This tool is used
  - for determining the data source of a DNS server

    - Notifies the continuous process of DNS server

- **Hmap**: This tool is used
    - To get the fingerprinting of web servers
        - to identify the version of server, vender of the server, model of the server and more
- **Nmap**: This tool is used
    - to scan the port address of the network,
    - It takes the fingerprint of operating system version, service and it can scan the network rapidly (http://insecure.org/nmap).

Scanning and scrutinizing gathered Information

- **Objectives of scanning:**
    - Port Scanning : Where information goes in and out of a computer
    - Identify open/close ports and services
    - Network Scanning: Understand IP addresses and computer network systems information.
    - Vulnerability Scanning: Understand the existing weaknesses in the system.
- Scrutinizing : “Enumeration”
    - Objectives:
    - 1. Valid user or group
    - Network resources and /or shared resources
    - OS and different applications that are running on the OS

- **Objectives of scanning:**
    - Port Scanning : Where information goes in and out of a computer
    - Identify open/close ports and services
    - Network Scanning: Understand IP addresses and computer network systems information.
    - Vulnerability Scanning: Understand the existing weaknesses in the system.
- Scrutinizing : “Enumeration”
    - Objectives:
    - 1. Valid user or group
    - Network resources and /or shared resources
    - OS and different applications that are running on the OS

Launch the Attack

- After scan and enumeration, the attack is launched using the following steps:
  - Crack the password
  - Exploit the privileges
  - Execute the malicious commands/applications
  - Hide the files
  - Cover the tracks like delete the access logs.
- Note:
  - The attackers spend 90% of the time in Reconnaissance, Scanning and scrutinizing on a target.
  - Only 10% of the time in launching the attack.

Social Engineering

- It is a way for criminals to gain access to information systems.
- The purpose of social engineering is usually to secretly install spyware, other malicious software or to trick persons into handing over passwords and/or other sensitive financial or personal information

What are they looking for

- Obtaining simple information such as your pet's name, where you're from, the places you've visited; information that you'd give out freely to your friends.
- Take a close look at some of the 'secure' sites you log into. Some have a 'secret question' you have to answer, if you cannot remember your username or password. The questions seem pretty tough for an outsider looking into trying to hack into your account.
    - What's the name of your first pet?
    - What is your maiden name?
    - When was your mother/father born?
    - Where were you born?

  Do these sound familiar?

- ➢ It is the “technique to influence” and “persuasion to deceive” people to obtain the information or perform some action.
- ➢ Social engineers exploit the natural tendency of a person to trust social engineers’ word, rather than exploiting computer security holes.
- ➢ Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders.

- The sign of truly successful social engineers is that they receive information without any suspicion.

Classification of Social Engineering

1. *Human-Based Social Engineering*

Human-based social engineering refers to person-to-person interaction to get the required/desired information.

2. *Computer-Based Social Engineering*

Computer-based social engineering refers to an attempt made to get the required/desired information by using computer software/Internet.

1. **Human Based (Non Technical)**
    1. Impersonating an employee or valid user : Posing employee of same organisation.
    2. Posing as an important user : Pretend to be an important user
    3. Using a third person : By authorised source to use system
    4. Calling technical support : By using Help desk
    5. Shoulder surfing : By watching over a person shoulder
    6. Dumpster diving : Looking in trash for information

2. Computer Based Social Engineering

1. Fake EMails
2. Email Attachments
3. Pop-up Windows

Protecting Yourself from Social Engineering Attack

1. Network defenses to repel virus
    - Virus protection (McAfee, Norton, Symantec, etc…)
    - Email attachment scanning
    - Firewalls, etc…
2. Organizations must decide what information is sensitive
3. Security must be periodically tested
4. Contact your security office immediately if you have any concerns at work

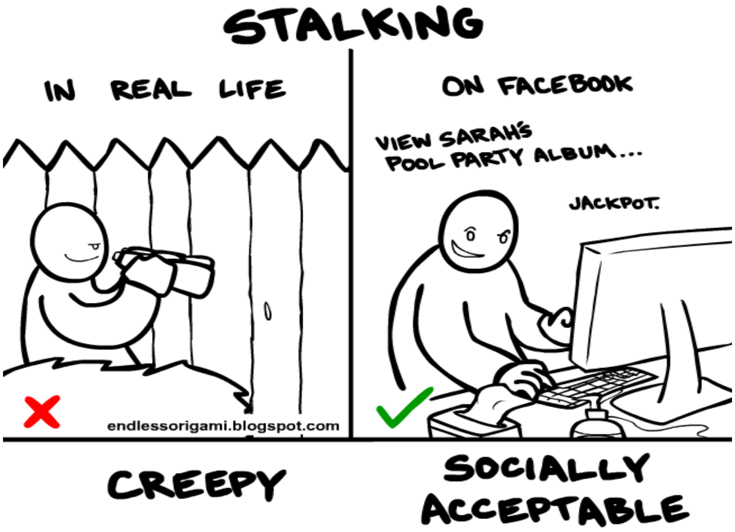
Cyber Stalking

Definition:

It is a crime in which the attacker harasses a victim using electronic communication, such as e-mail or instant messaging (IM), or messages posted to a Web site or a discussion group.

Stalking:

- A cyber stalker relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected.



- Cyberstalking messages differ from ordinary spam.
- Cyber stalker targets a specific victim with often threatening messages, while the spammer targets a multitude of recipients with simply annoying messages.

Types of Stalkers

- Mainly 2 types :
    - Online Stalkers :
        - Def: Interaction with the victim using Internet.
        - Ex: Email, Chat
    - Offline Stalkers:
        - Def: Begin the attack using traditional methods.
        - Ex: Watching daily, Personal websites.

Other types :

- The four most important types are:
    - Rejected Stalker
    - Resentful Stalker
    - Predatory Stalker
    - Intimacy Stalker

Rejected Stalker

- Most common, persistent, and intrusive
- Obsessed with someone who is a former romantic partner or friend, and who has ended their relationship, or indicates that he or she intends to end the relationship.

Resentful Stalker

- Looking for revenge against someone who has upset them--it could be someone known to the stalker or a complete stranger.
    - Their behaviors are meant to frighten and distress the victim

Predatory Stalker

- Least common
- Are a classic sexual predator whose plan is to physically or sexually attack the victim.
- Their motivated purely by the desire for sexual gratification and power over their victim

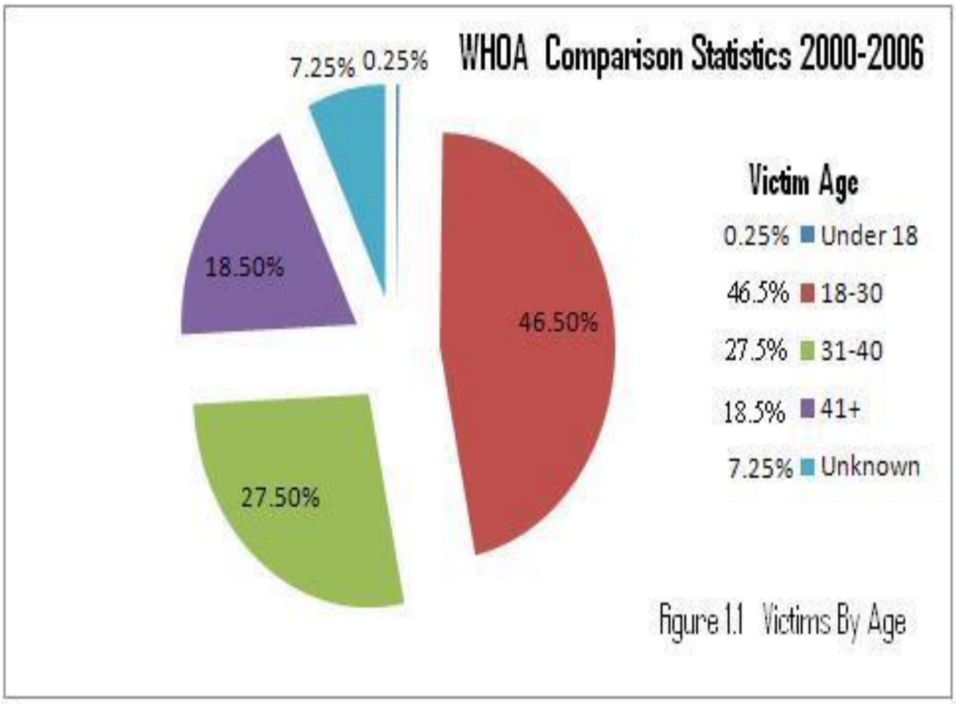
Intimacy Stalker

- They seeks to establish an intimate, loving relationship with their victim.

    The victim and himself were “meant to be together.”

- These types of people think that the victim owes them love and affection because of all the time and effort it took for the stalker to stalk them.

Analysis…

- The majority of cyberstalkers are men and the majority of their victims are women but…..
- Jane A. Hitchcock, president of WHOA says, “The most surprising thing we've seen is the rise in female cyberstalkers - this increased from 27% in 2000 to 35% in 2002 to 38% in 2003.”
- According to the Working to Halt Online Abuse (WHOA) from 2000 to 2006, out of the total cases, 2036, of cyberstalking….
- 

How stacking works?

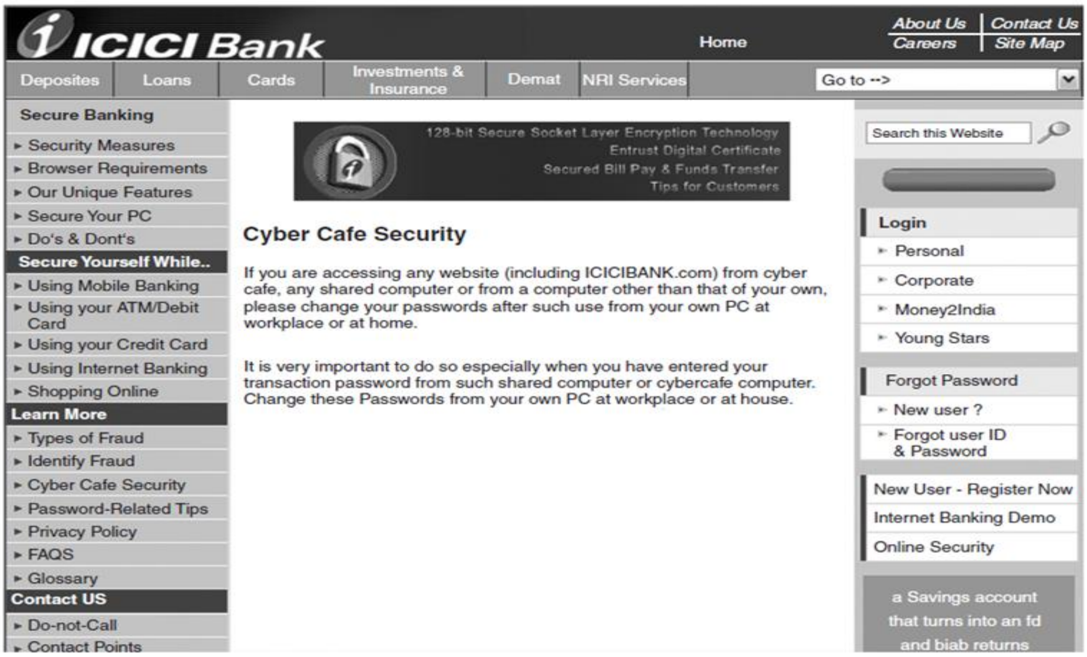
- In the following way

1. Personal information gathering about the victim.
    - Ex: Name, background, contact number, etc.
2. Establish a contact with victim through phone.
3. Stalkers will almost always establish a contact with the victims through EMail.
4. Some stalkers keep on sending repeated E-mail.
5. Post victims personal information on any illicit services website
6. Who were received information , start calling the victims on the given contact details.
7. Stalkers subscribe/register the E-mail account of the victim to pornographic and sex sites.

1. Real Life Incident:
    – Case study: In Delhi, 40 calls in 3 days.

Cybercafe and Cybercrimes

- Cybercrimes such as stealing of bank passwords and subsequent fraudulent withdrawal of money have also happened through cybercafes.
- Cybercafes have also been used regularly for sending obscene mails to harass people.
- Indian Information Technology Act (ITA) 2000 interprets cybercafes as “network service providers” referred to under the erstwhile Section 79, which imposed on them a responsibility for “due diligence” failing which they would be liable for the offenses committed in their network.

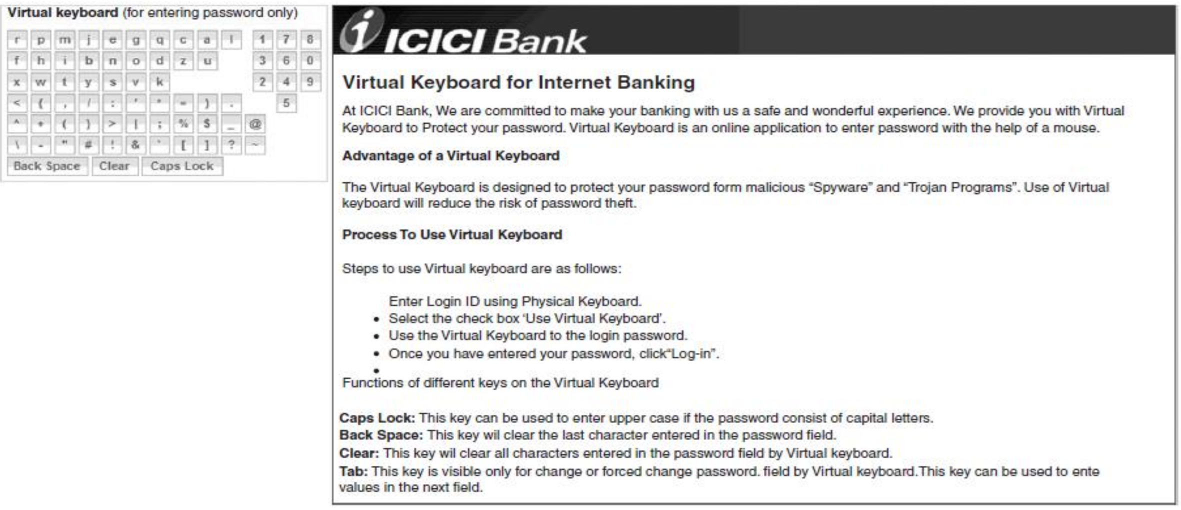


Cyber Cafe Security

If you are accessing any website (including ICICIBANK.com) from cyber cafe, any shared computer or from a computer other than that of your own, please change your passwords after such use from your own PC at workplace or at home.

It is very important to do so especially when you have entered your transaction password from such shared computer or cybercafe computer. Change these Passwords from your own PC at workplace or at house.

Figure 1 Cybercafe security.
Source: http://www.icicibank.com/pfsuser/temp/cybersec.htm (27 June 2009).



Virtual Keyboard for Internet Banking

At ICICI Bank, We are committed to make your banking with us a safe and wonderful experience. We provide you with Virtual Keyboard to Protect your password. Virtual Keyboard is an online application to enter password with the help of a mouse.

Advantage of a Virtual Keyboard

The Virtual Keyboard is designed to protect your password form malicious “Spyware” and “Trojan Programs”. Use of Virtual keyboard will reduce the risk of password theft.

Process To Use Virtual Keyboard

Steps to use Virtual keyboard are as follows:

Enter Login ID using Physical Keyboard.
- Select the check box ‘Use Virtual Keyboard’.
- Use the Virtual Keyboard to the login password.
- Once you have entered your password, click“Log-in”.
-

Functions of different keys on the Virtual Keyboard

Caps Lock: This key can be used to enter upper case if the password consist of capital letters.
Back Space: This key wil clear the last character entered in the password field.
Clear: This key wil clear all characters entered in the password field by Virtual keyboard.
Tab: This key is visible only for change or forced change password. field by Virtual keyboard.This key can be used to ente values in the next field.

Figure 2 Virtual keyboard.
Source: http://www.icicibank.com/pfsuser/webnews/virtualkeyboad.htm (27 June 2009).

Cybercriminals can either install malicious programs such as keyloggers and/or Spyware or launch an attack on the target.

Here are a few tips for safety and security while using the computer in a cybercafe:

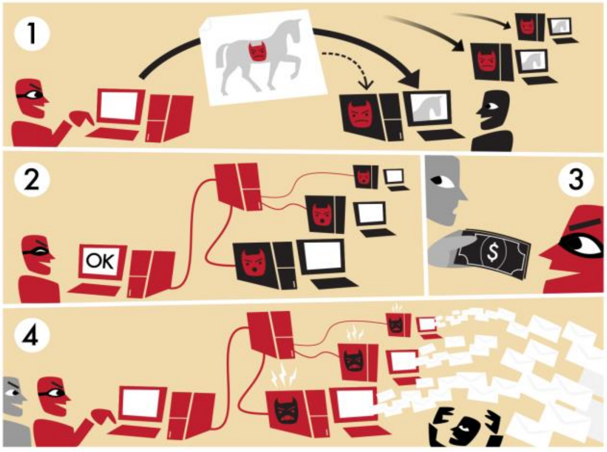
1. Always logout
2. Stay with the computer
3. Clear history and temporary files
4. Be alert
5. Avoid online financial transactions
6. Change passwords
7. Virtual keyboard
8. Security warnings
9.

Botnet: The fuel of Cybercrime

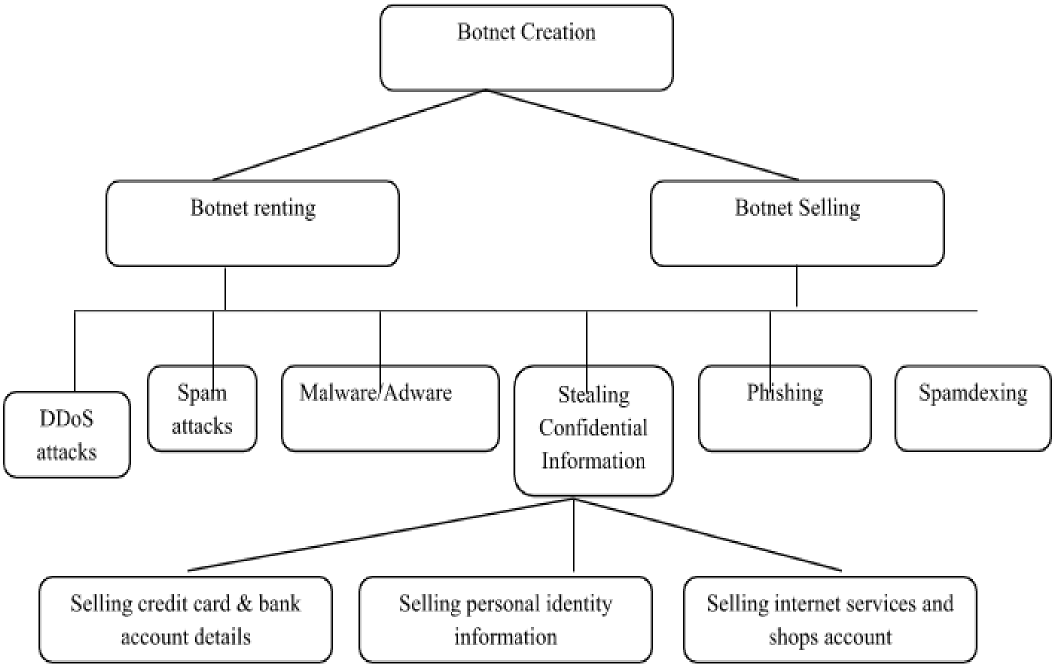
- A Botnet (also called as zombie network) is a network of computers infected with a malicious program that allows cybercriminals to control the infected machines remotely without the users' knowledge.
- Your computer system maybe a part of a Botnet even though it appears to be operating normally.
- Botnets are often used to conduct a range of activities, from distributing Spam and viruses to conducting denial-of-service (DoS) attacks.

Evolution of Botnets

- Motivation change in computer hacking
    - Vandalism Financial gains
    - Loss of $67.2 billion (2006 figure)



How botnets creates the business


Botnet Creation
Botnet renting
Botnet Selling
DDoS attacks
Spam attacks
Malware/Adware
Stealing Confidential Information
Phishing
Spamdexing
Selling credit card & bank account details
Selling personal identity information
Selling internet services and shops account

One can ensure following to secure the system:

1. Use antivirus and anti-Spyware software and keep it up-to-date.
2. Set the OS to download and install security patches automatically.
3. Use a firewall to protect the system from hacking attacks while it is connected on the Internet.
4. Disconnect from the Internet when you are away from your computer.
5. Downloading the freeware only from websites that are known and trustworthy
6. Check regularly the folders in the mail box – "sent items" or "outgoing" – for those messages you did not send.
7. Take an immediate action if your system is infected.

Attack Vector

- An "attack vector" is a path or means by which an attacker can gain access to a computer or to a network server to deliver a payload or malicious outcome.
- Attack vectors include viruses, E-Mail attachments, webpages, pop-up windows, instant messages, chat rooms, and deception.
- The most common malicious payloads are viruses, Trojan Horses, worms, and Spyware.
- If an attack vector is thought of as a guided missile, its payload can be compared to the warhead in the tip of the missile.

- ✓ Payload means the malicious activity that the attack performs.
- ✓ It is the bits that get delivered to the end-user at the destination.

The attack vectors described here are how most of them are launched:

1. Attack by EMail
2. Attachments (and other files)
3. Attack by deception
4. Hackers
5. Heedless guests (attack by webpage)
6. Attack of the worms
7. Malicious macros
8. Foistware (sneakware)
9. Viruses

Cloud Security

Cloud computing services, while offering considerable benefits and cost savings makes it easier for cybercriminals to attack these systems.

Cloud computing is Internet (“cloud”)-based development and use of computer technology (“computing”).

A cloud service has three distinct characteristics which differentiate it from traditional

hosting:

1. It is sold on demand
2. it is elastic in terms of usage
3. the service is fully managed by the provider.

Advantages of Cloud Computing

4. Cloud computing has following advantages:
5. 1. Applications and data can be accessed from anywhere at any time.
6. 2. It could bring hardware costs down.
7. 3. Organizations do not have to buy a set of software or software licenses for every employee and the organizations could pay a metered fee to a cloud computing company.
8. 4. Organizations do not have to rent a physical space to store servers and databases. Servers and digital storage devices take up space.
9. 5. Organizations would be able to save money on IT support because organizations will have to ensure about the desktop (i.e., a client) and continuous Internet connectivity instead of servers and other hardware.

The cloud computing services can be either private or public.

- A public cloud sells services to anyone on the Internet.
- A private cloud is like a proprietary network or a data center that supplies the hosted services to a limited number of people.

Types of Services

Services provided by cloud computing are as follows:

1. Infrastructure-as-a-service (IaaS)
2. Platform-as-a-service (PaaS)
3. Software-as-a-service (SaaS)

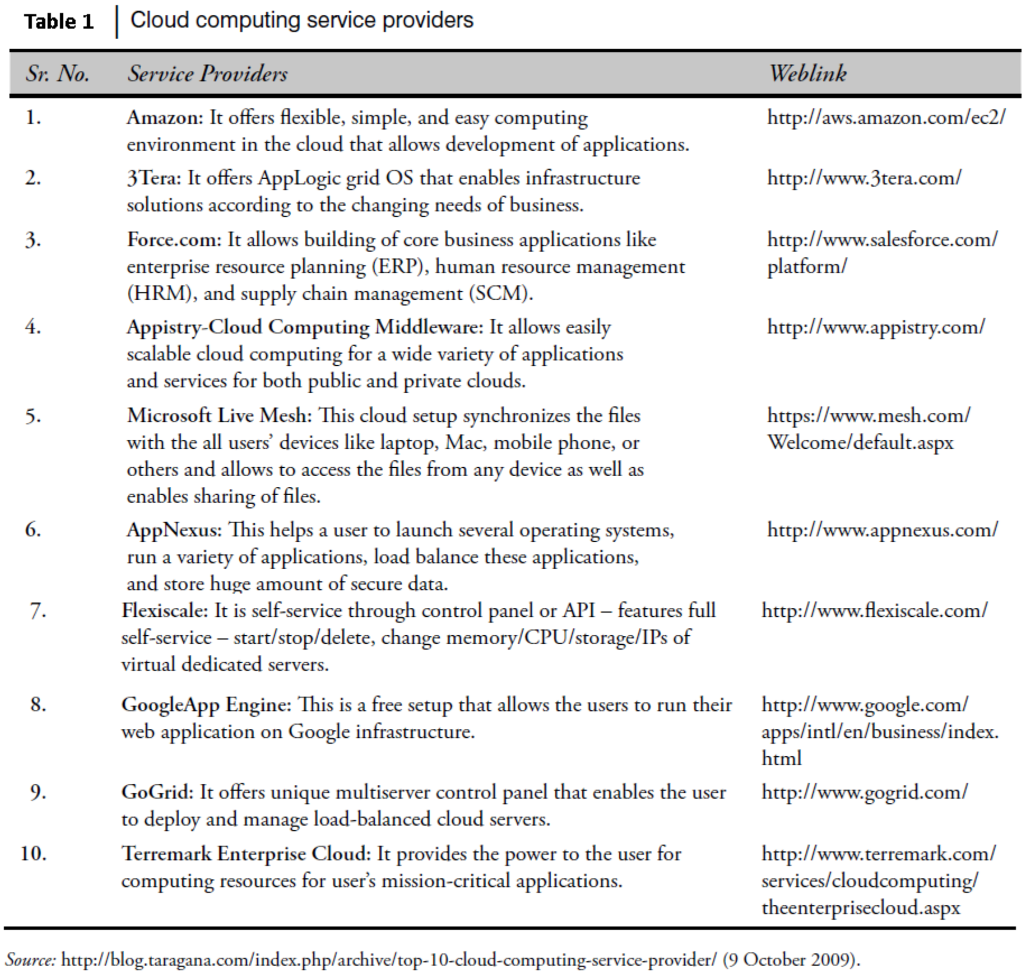


Table 1 | Cloud computing service providers

Sr. No.	*Service Providers*	*Weblink*
1.	**Amazon:** It offers flexible, simple, and easy computing environment in the cloud that allows development of applications.	http://aws.amazon.com/ec2/
2.	**3Tera:** It offers AppLogic grid OS that enables infrastructure solutions according to the changing needs of business.	http://www.3tera.com/
3.	**Force.com:** It allows building of core business applications like enterprise resource planning (ERP), human resource management (HRM), and supply chain management (SCM).	http://www.salesforce.com/platform/
4.	**Appistry-Cloud Computing Middleware:** It allows easily scalable cloud computing for a wide variety of applications and services for both public and private clouds.	http://www.appistry.com/
5.	**Microsoft Live Mesh:** This cloud setup synchronizes the files with the all users' devices like laptop, Mac, mobile phone, or others and allows to access the files from any device as well as enables sharing of files.	https://www.mesh.com/Welcome/default.aspx
6.	**AppNexus:** This helps a user to launch several operating systems, run a variety of applications, load balance these applications, and store huge amount of secure data.	http://www.appnexus.com/
7.	**Flexiscale:** It is self-service through control panel or API – features full self-service – start/stop/delete, change memory/CPU/storage/IPs of virtual dedicated servers.	http://www.flexiscale.com/
8.	**GoogleApp Engine:** This is a free setup that allows the users to run their web application on Google infrastructure.	http://www.google.com/apps/intl/en/business/index.html
9.	**GoGrid:** It offers unique multiserver control panel that enables the user to deploy and manage load-balanced cloud servers.	http://www.gogrid.com/
10.	**Terremark Enterprise Cloud:** It provides the power to the user for computing resources for user's mission-critical applications.	http://www.terremark.com/services/cloudcomputing/theenterprisecloud.aspx

Source: http://blog.taragana.com/index.php/archive/top-10-cloud-computing-service-provider/ (9 October 2009).

Cybercrime and Cloud Computing

Prime area of the risk in cloud computing is protection of user data.

Table 2 shows the major areas of concerns in cloud computing domain.

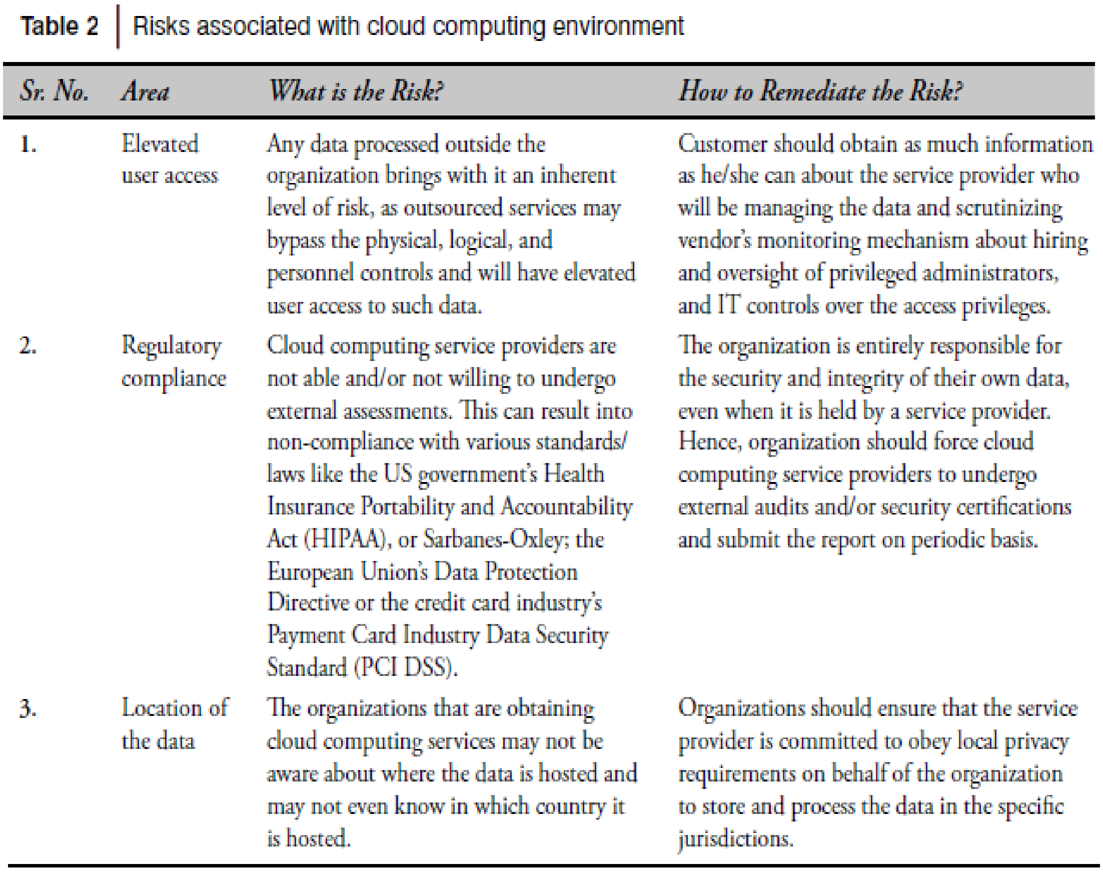
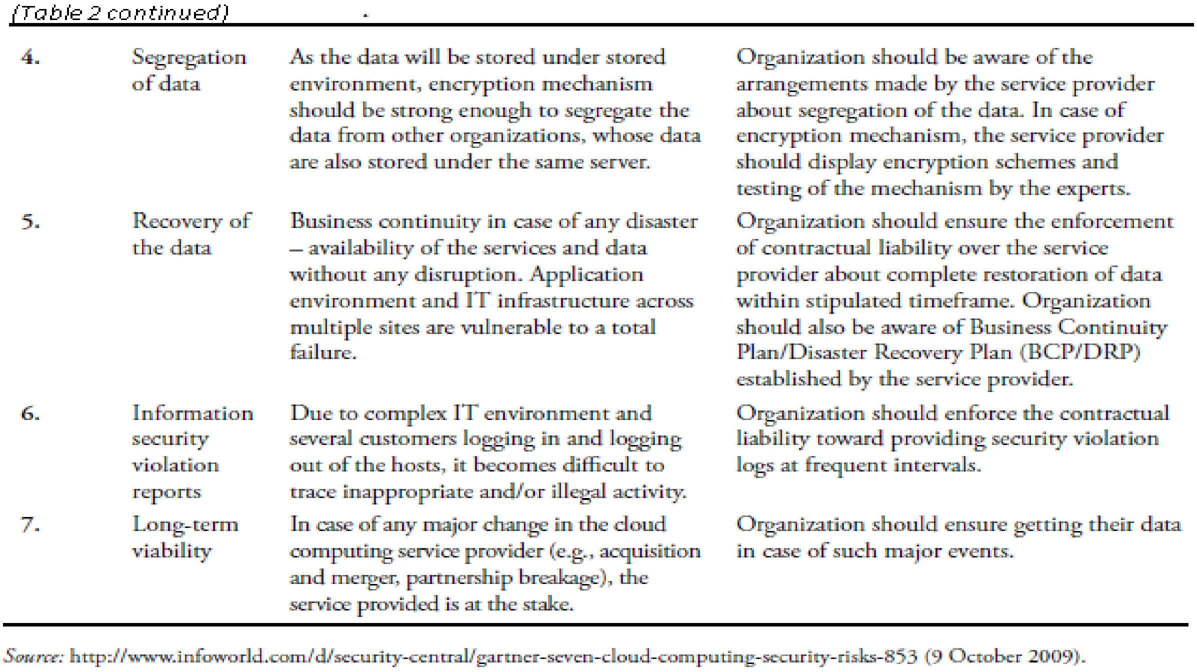


Table 2 | Risks associated with cloud computing environment

Sr. No.	*Area*	*What is the Risk?*	*How to Remediate the Risk?*
1.	Elevated user access	Any data processed outside the organization brings with it an inherent level of risk, as outsourced services may bypass the physical, logical, and personnel controls and will have elevated user access to such data.	Customer should obtain as much information as he/she can about the service provider who will be managing the data and scrutinizing vendor's monitoring mechanism about hiring and oversight of privileged administrators, and IT controls over the access privileges.
2.	Regulatory compliance	Cloud computing service providers are not able and/or not willing to undergo external assessments. This can result into non-compliance with various standards/ laws like the US government's Health Insurance Portability and Accountability Act (HIPAA), or Sarbanes-Oxley; the European Union's Data Protection Directive or the credit card industry's Payment Card Industry Data Security Standard (PCI DSS).	The organization is entirely responsible for the security and integrity of their own data, even when it is held by a service provider. Hence, organization should force cloud computing service providers to undergo external audits and/or security certifications and submit the report on periodic basis.
3.	Location of the data	The organizations that are obtaining cloud computing services may not be aware about where the data is hosted and may not even know in which country it is hosted.	Organizations should ensure that the service provider is committed to obey local privacy requirements on behalf of the organization to store and process the data in the specific jurisdictions.

(Continued)

(Table 2 continued)



4.	Segregation of data	As the data will be stored under stored environment, encryption mechanism should be strong enough to segregate the data from other organizations, whose data are also stored under the same server.	Organization should be aware of the arrangements made by the service provider about segregation of the data. In case of encryption mechanism, the service provider should display encryption schemes and testing of the mechanism by the experts.
5.	Recovery of the data	Business continuity in case of any disaster – availability of the services and data without any disruption. Application environment and IT infrastructure across multiple sites are vulnerable to a total failure.	Organization should ensure the enforcement of contractual liability over the service provider about complete restoration of data within stipulated timeframe. Organization should also be aware of Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) established by the service provider.
6.	Information security violation reports	Due to complex IT environment and several customers logging in and logging out of the hosts, it becomes difficult to trace inappropriate and/or illegal activity.	Organization should enforce the contractual liability toward providing security violation logs at frequent intervals.
7.	Long-term viability	In case of any major change in the cloud computing service provider (e.g., acquisition and merger, partnership breakage), the service provided is at the stake.	Organization should ensure getting their data in case of such major events.

Source: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853 (9 October 2009).

Unit-3

Cryptography and Cryptanalysis

Introduction to Cryptography

- Cryptography: process of making and using codes to secure transmission of information
- Encryption: converting original message into a form unreadable by unauthorized individuals
- Cryptanalysis: process of obtaining original message from encrypted message without knowing algorithms or keys
- Cryptology: science of encryption; combines cryptography and cryptanalysis
- Cryptosystem: A System for encryption and decryption is called as cryptosystem.

Need of Encryption

- Confidentiality
- Integrity
- Authentication
- Non repudiation
- Access control
- Availability

Cipher Methods

- Plaintext can be encrypted through bit stream or block cipher method
- Bit stream: each plaintext bit transformed into cipher bit one bit at a time
- Block cipher: message divided into blocks (e.g., sets of 8- or 16-bit blocks) and each is transformed into encrypted block of cipher bits using algorithm and key

Techniques of Cryptography

- Substitution cipher: substitute one value for another
    - Monoalphabetic substitution: uses only one alphabet
    - Polyalphabetic substitution: more advanced; uses two or more alphabets
    - Vigenère cipher: advanced cipher type that uses simple polyalphabetic code; made up of 26 distinct cipher alphabets
    - Transposition cipher: rearranges values within a block to create ciphertext
        - Exclusive OR (XOR): function of Boolean algebra; two bits are compared
        - If two bits are identical, result is binary 0
        - If two bits not identical, result is binary 1

- Vernam cipher: developed at AT&T; uses set of characters once per encryption process
- Book (running key) cipher: uses text in book as key to decrypt a message; ciphertext contains codes representing page, line, and word numbers
- Hash Functions: Mathematical algorithms that generate message summary/digest to confirm message identity and confirm no content has changed

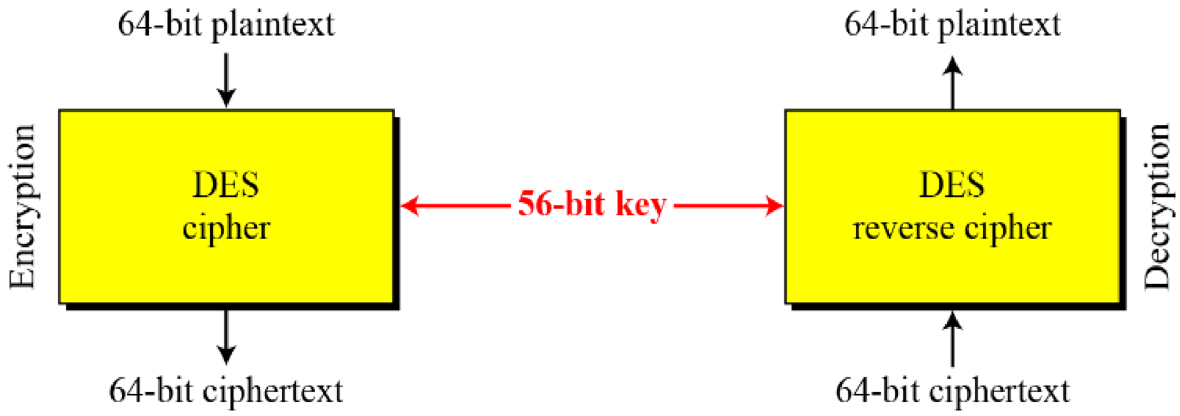
Cryptographic Algorithms

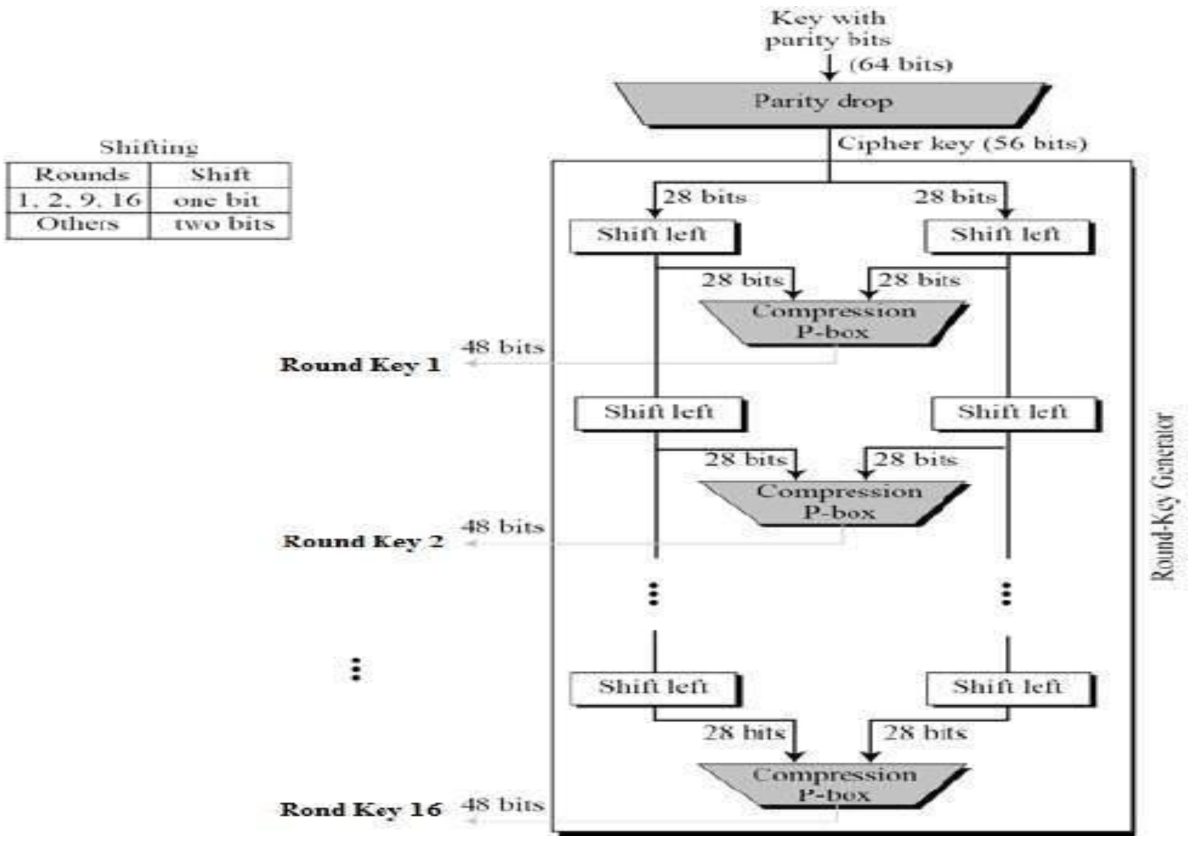
- Often grouped into two broad categories, symmetric and asymmetric; today's popular cryptosystems use hybrid combination of symmetric and asymmetric algorithms
- Symmetric and asymmetric algorithms are distinguished by types of keys used for encryption and decryption operations.
- Symmetric encryption: uses same "secret key" to encipher and decipher message
- Encryption methods can be extremely efficient, requiring minimal processing
- Both sender and receiver must possess encryption key
- If either copy of key is compromised, an intermediate can decrypt and read messages

Symmetric Key Cryptography

- DES: Data Encryption Standards
- The Data Encryption Standard(DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology(NIST).
- History

In1973, NIST published a request for proposals for a national symmetric-key cryptosystem. A proposal from IBM, a modification of a project called Lucifer, was accepted as DES. DES was published in the Federal Register in March 1975 as a draft of the Federal Information Processing Standard(FIPS).



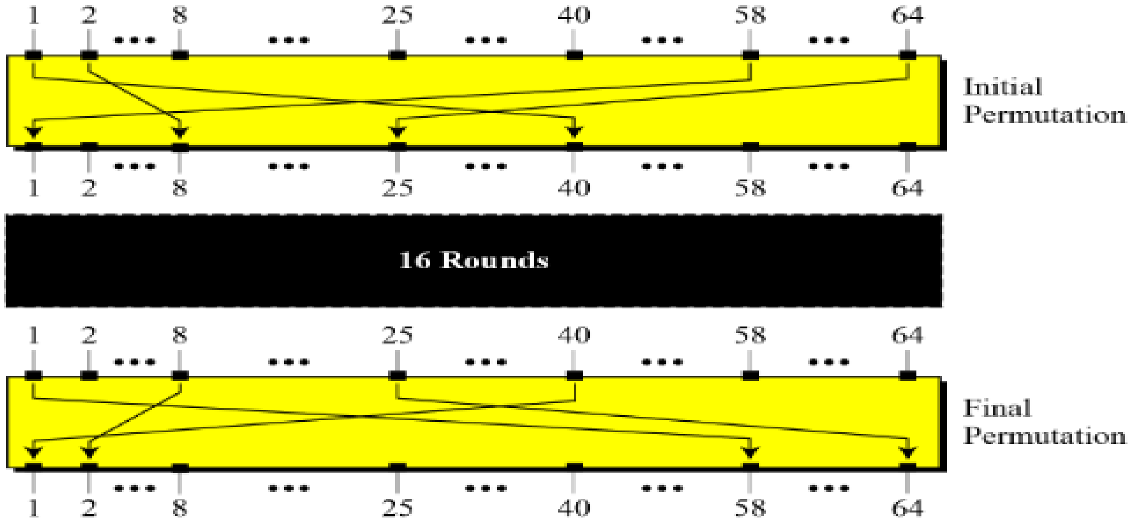


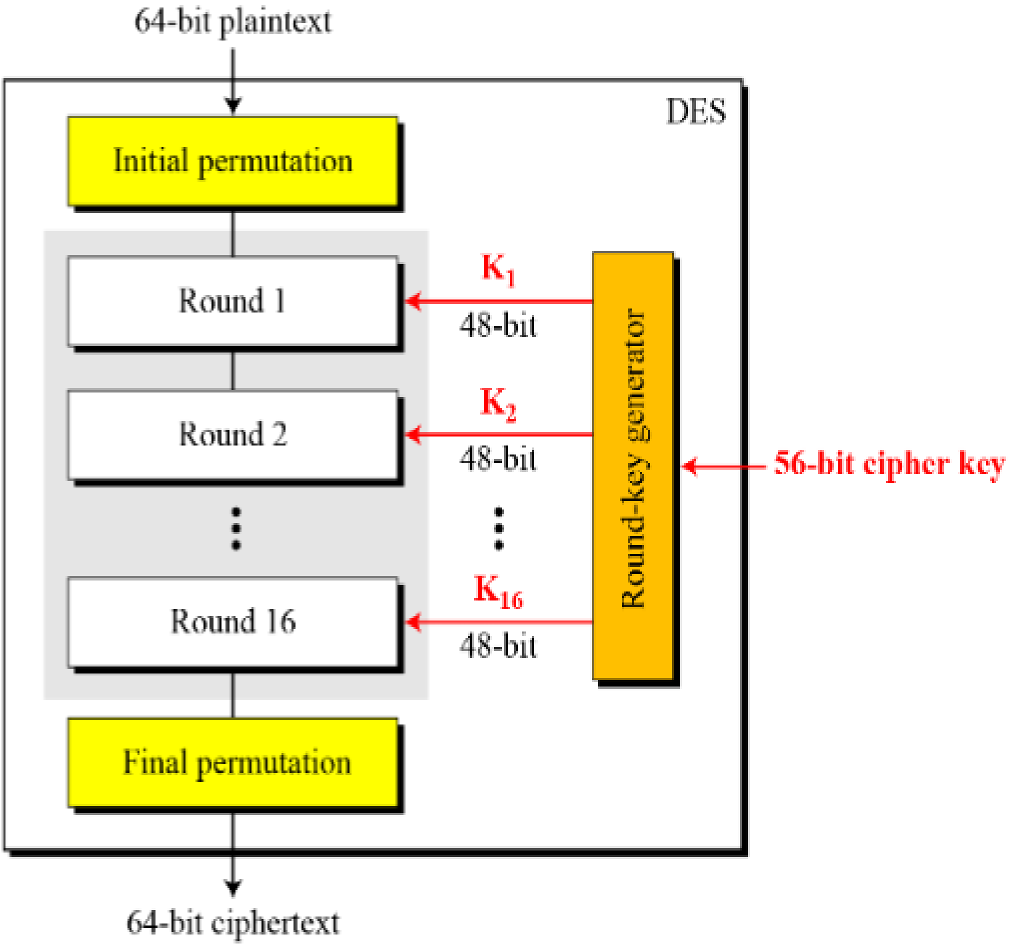
DES STRUCTURE

The encryption process is made of two permutations (P-boxes), which we call initial and final permutations, and sixteen Feistel rounds.

- Initial and Final Permutations
- Rounds
- Cipher and Reverse Cipher
- Examples

Initial and Final Permutations





Initial and final permutation

Table 6.1 ***Initial and final permutation tables***

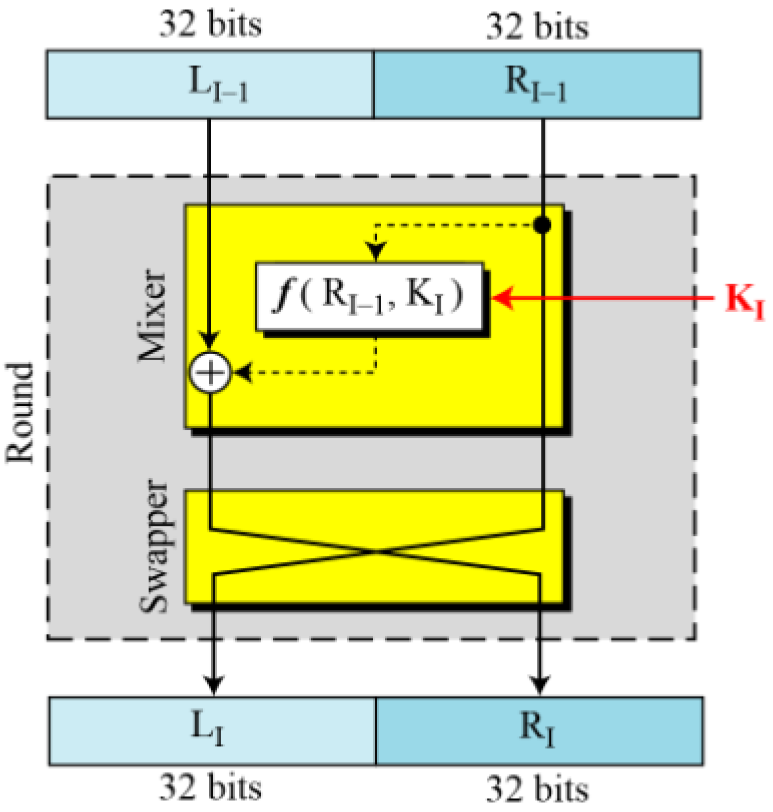
Initial Permutation	*Final Permutation*
58 50 42 34 26 18 10 02	40 08 48 16 56 24 64 32
60 52 44 36 28 20 12 04	39 07 47 15 55 23 63 31
62 54 46 38 30 22 14 06	38 06 46 14 54 22 62 30
64 56 48 40 32 24 16 08	37 05 45 13 53 21 61 29
57 49 41 33 25 17 09 01	36 04 44 12 52 20 60 28
59 51 43 35 27 19 11 03	35 03 43 11 51 19 59 27
61 53 45 37 29 21 13 05	34 02 42 10 50 18 58 26
63 55 47 39 31 23 15 07	33 01 41 09 49 17 57 25

The initial and final permutations are straight P-boxes that are inverses of each other.They have no cryptography significance in DES.

Rounds

DES uses 16 rounds. Each round of DES is a Feistel cipher.

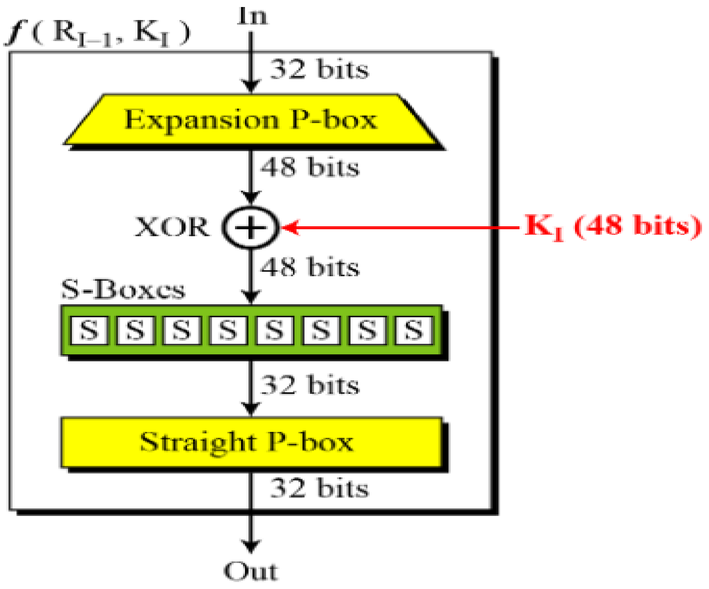
Figure 6.4
A round in DES (encryption site)



DES Function

The heart of DES is the DES function. The DES function applies a 48-bit key to the right most 32bits to produce a 32-bit output.

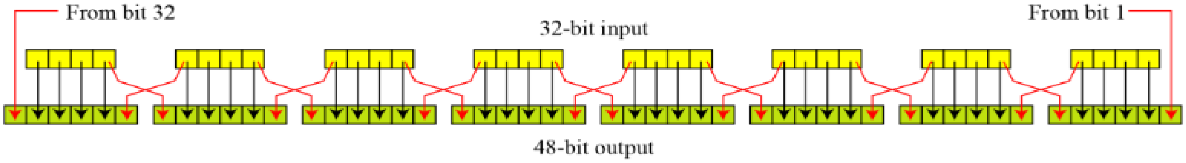
Figure 6.5
DES function



Expansion P-box

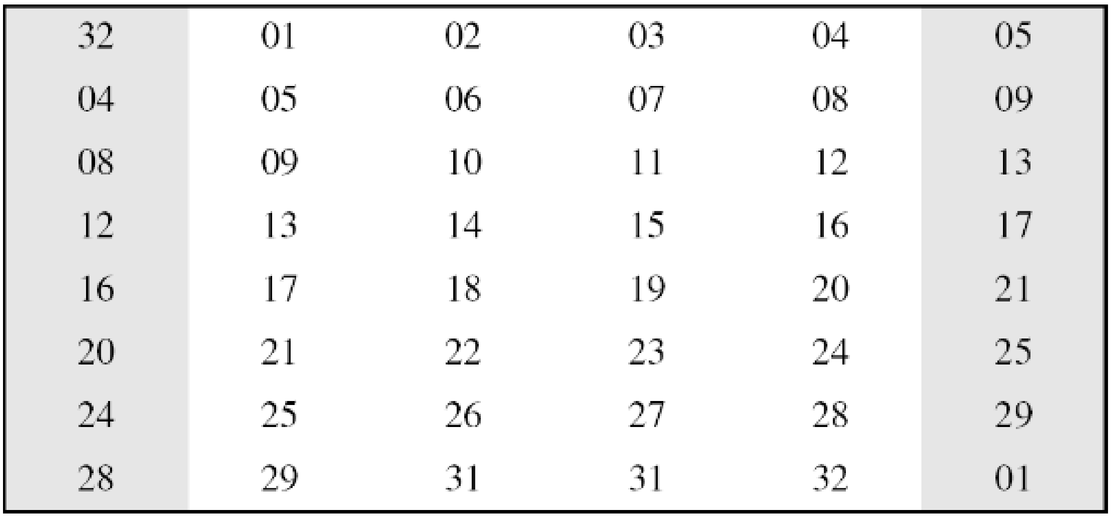
Since RI−1 is a 32-bit input and KI is a 48-bit key, we first need to expand RI−1 to 48bits

Figure 6.6 ***Expansion permutation***



Although the relationship between the input and output can be defined mathematically, DES uses to define this P-box

Table 6.6 ***Expansion P-box table***



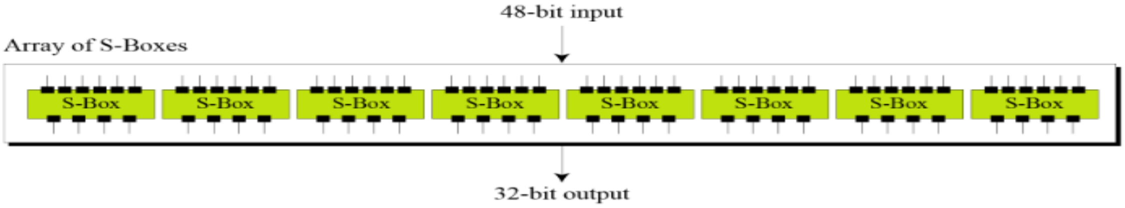
32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

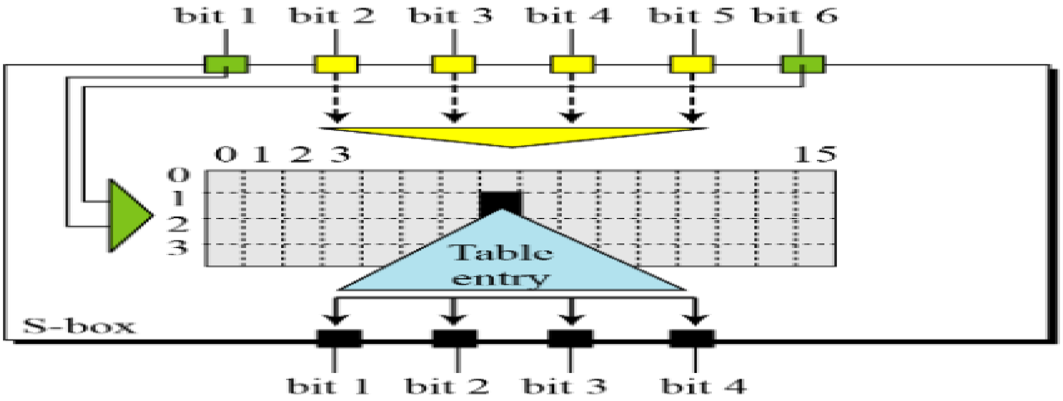
Whitener (XOR)

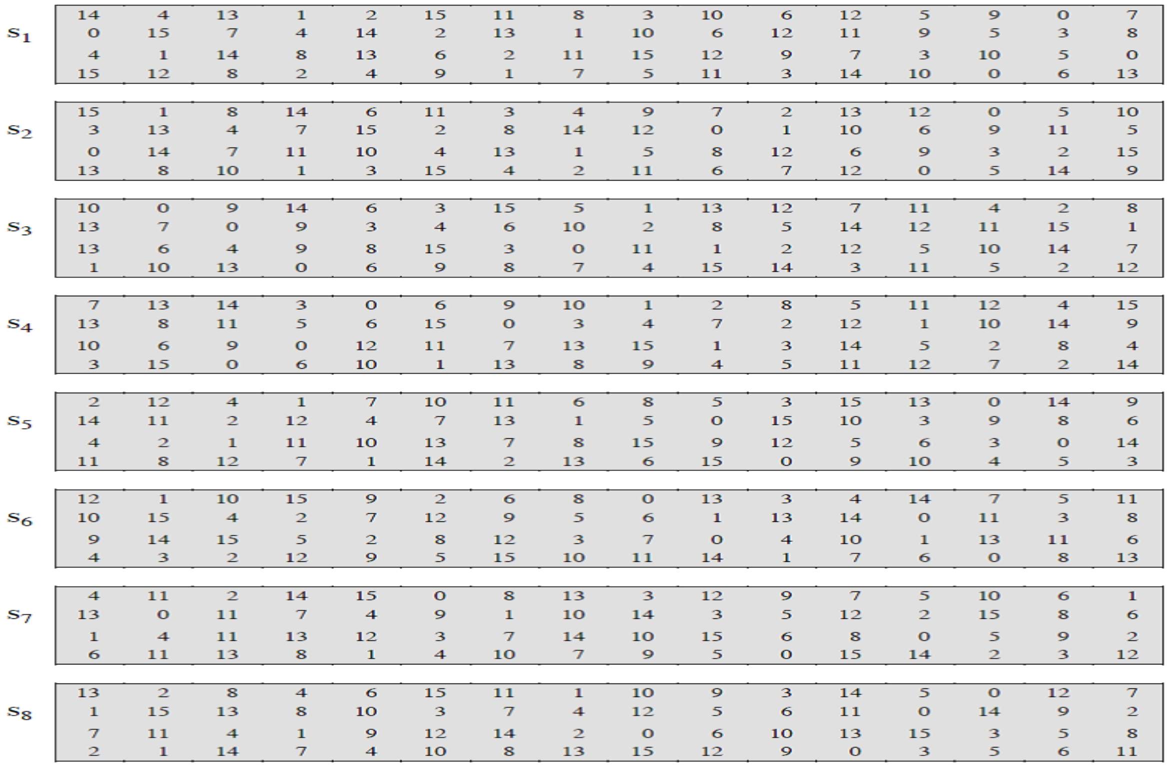
After the expansion permutation, DES uses the XOR operation on the expanded right section and the round key. Note that both the right section and the key are 48-bits in length. Also note that the round key is used only in this operation.

S-Boxes

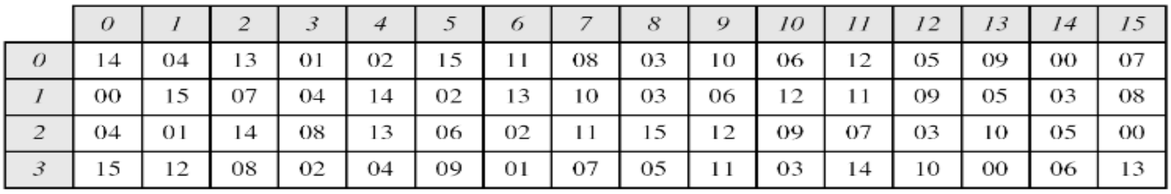
The S-boxes do the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output.





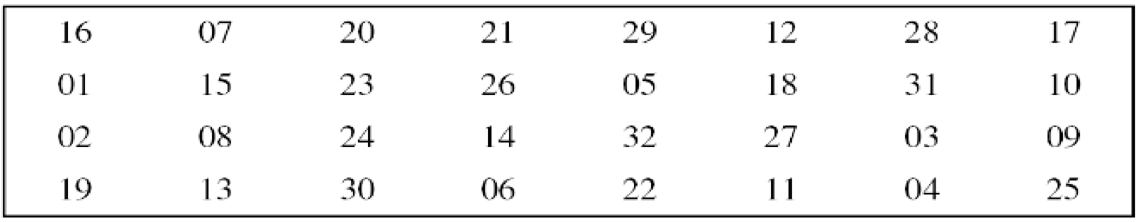


S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

Straight Permutation



16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

Cipher and Reverse Cipher

Using mixers and swappers, we can create the cipher and reverse cipher, each having 16 rounds

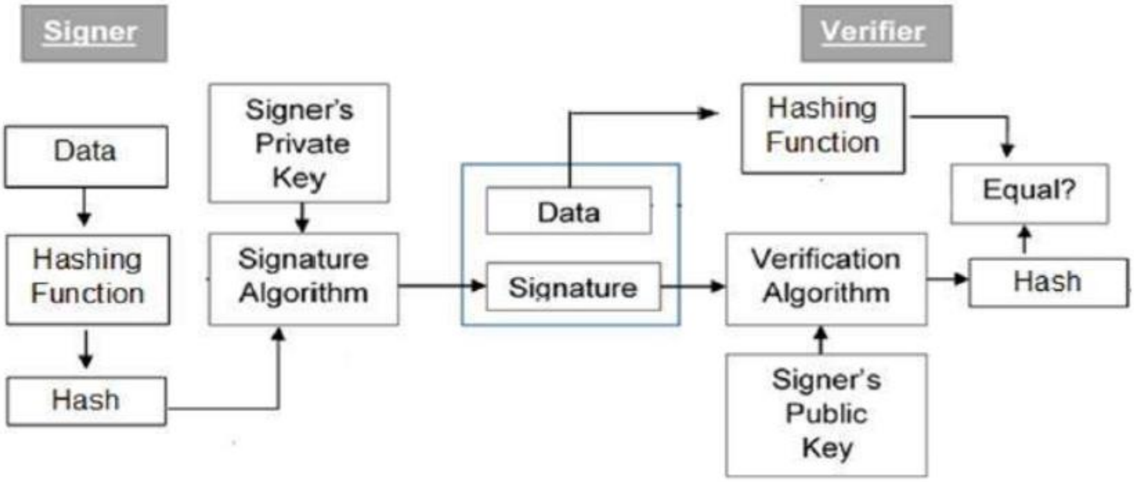
Cipher First Approach To achieve this goal, one approach is to make the last round(round16) different from the others; it has only a mixer and no swapper.

Digital Signatures

- Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.
- Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.
- Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

Model of Digital Signature

The digital signature scheme is based on public key cryptography. The model of digital signature scheme is depicted in the following illustration –

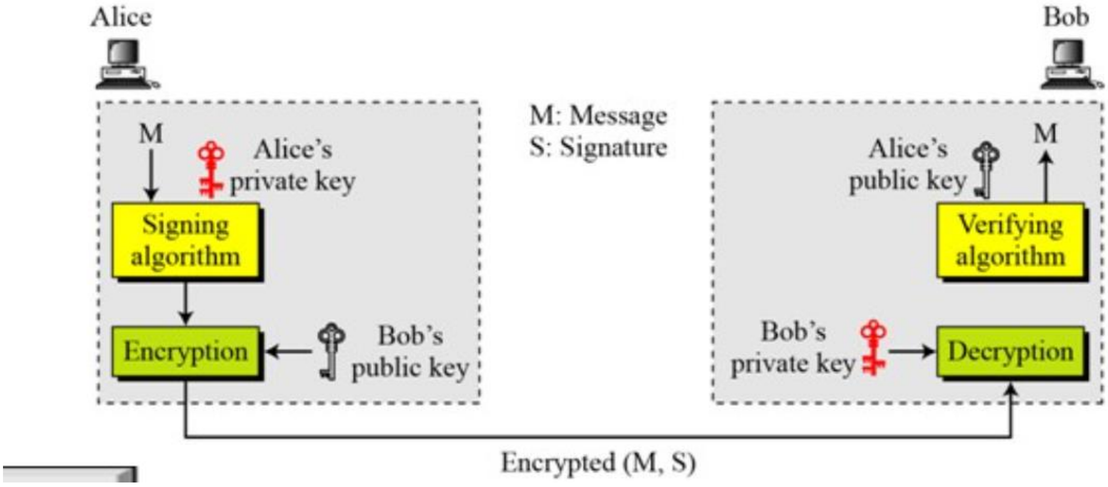


The following points explain the entire process in detail –

- Each person adopting this scheme has a public-private key pair.
- Generally, the key pairs used for encryption/decryption and signing/verifying are different. The private key used for signing is referred to as the signature key and the public key as the verification key.

- Signer feeds data to the hash function and generates hash of data.
- Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. Signature is appended to the data and then both are sent to the verifier.
- Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output.
- Verifier also runs same hash function on received data to generate hash value.
- For verification, this hash value and output of verification algorithm are compared. Based on the comparison result, verifier decides whether the digital signature is valid.
- Since digital signature is created by ‘private’ key of signer and no one else can have this key; the signer cannot repudiate signing the data in future.

Figure 13.5 *Adding confidentiality to a digital signature scheme*



Importance of Digital Signature

Out of all cryptographic primitives, the digital signature using public key cryptography is considered as very important and useful tool to achieve information security.

Apart from ability to provide non-repudiation of message, the digital signature also provides message authentication and data integrity. Let us briefly see how this is achieved by the digital signature −

- Message authentication − When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.
- Data Integrity − In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.
- Non-repudiation − Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can

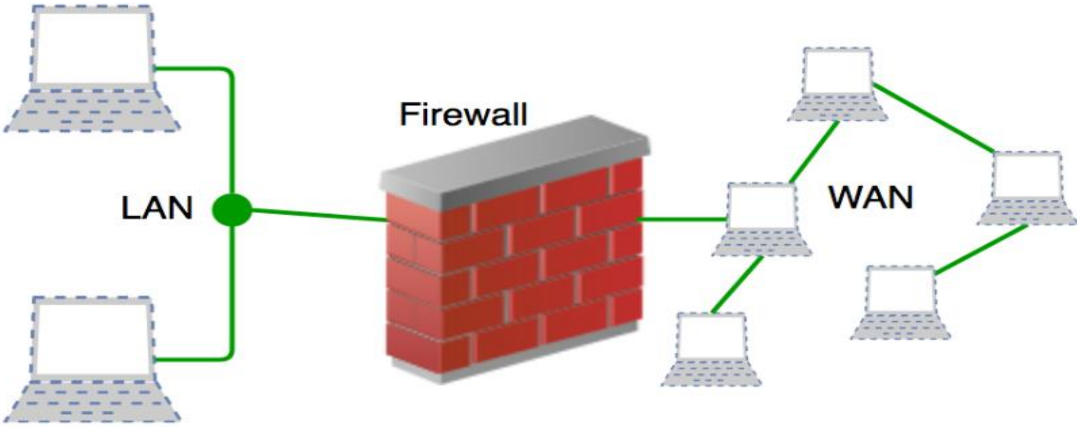
present data and the digital signature to a third party as evidence if any dispute arises in the future.

Applications of Cryptography

- There are various applications of cryptography which are as follows −
- Secrecy in Transmission − Some existing secrecy systems for transmission access a private key system for converting transmitted data because it is the quickest approach that functions with rational guarantee and low overhead.
    - If the multiple conversing parties is minute, key distribution is implemented periodically with a courier service and key preservation based on physical security of the keys over the method of use and destruction after new keys are disseminated.
- Secrecy in Storage − Secrecy in storage is frequently preserved by a one-key system where the user provide the key to the computer at the commencement of a session, and the system creates concern of encryption and decryption during the phase of normal use.
- Integrity in Transmission − Some users of communication systems are not as much worried concerning secrecy as about integrity. In a computer funds transfer, the sum sent from one account to another is usually public knowledge.
    - If an operating tapper can bring in a false transfer, funds can be shared illegally. An inaccuracy in an individual bit can cause millions of dollars to be wrongly credited or debited. Cryptographic methods are generally used to provide that intentional or accidental modification of transmitted data does not cause flawed actions to appear.
- Integrity in Storage − The central meaning of assuring integrity of accumulated data has previously been access control. Access control contains systems of locks and keys, guards, and other approaches of a physical or logical feature.
    - The recent advent of computer viruses has altered this to an important degree, and the use of cryptographic checksums for assuring the integrity of stored data is becoming broad.
- Authentication of Identity − Authenticating the identity of individuals or systems to each other has been a difficulty for a very long time. Simple passwords have been used to test identity. More compound protocols such as sequence of keywords exchanged between sets of parties are generally display in the movies or on television.
- Credentialing Systems − A credential is generally a file that introduces one party to another by referencing a usually known trusted party. When credit is used for, references are usually requested. The credit of the references is determined and they are contacted to discover out the tested of the applicant. Credit cards are generally used to credential an individual to achieve more credit cards.
- Electronic Signatures − Electronic signatures are a means of monetary a lawfully binding transaction among two or more parties. It can be as functional as a physical signature, electronic signatures should be at least as hard to fake at least as simple to use, and accepted in a court of law as binding upon some parties to the operation.

Overview of Firewalls

- A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.
- Accept : allow the traffic
  Reject : block the traffic but reply with an "unreachable error"
  Drop : block the traffic with no reply
- A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.



Firewall History

Firewalls have existed since the late 1980's and started out as packet filters, which were networks set up to examine packets, or bytes, transferred between computers. Though packet filtering firewalls are still in use today, firewalls have come a long way as technology has developed throughout the decades.

Gen 1 Virus

Generation 1, Late 1980's, virus attacks on stand-alone PC's affected all businesses and drove anti-virus products.

Gen 2 Networks

Generation 2, Mid 1990's, attacks from the internet affected all business and drove creation of the firewall.

Gen 3 Applications

Generation 3, Early 2000's, exploiting vulnerabilities in applications which affected most businesses and drove Intrusion Prevention Systems Products (IPS).

Gen 4 Payload

Generation 4, Approx. 2010, rise of targeted, unknown, evasive, polymorphic attacks which affected most businesses and drove anti-bot and sandboxing products.

Gen 5 Mega

Generation 5, Approx. 2017, large scale, multi-vector, mega attacks using advance attack tools and is driving advance threat prevention solutions.

What Firewalls Do?

Firewalls, and especially Next Generation Firewalls, focus on blocking malware and application-layer attacks, along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls can react quickly and seamlessly to detect and react to outside attacks across the whole network.

Types of Firewall

- There are mainly three types of firewalls, such as software firewalls, hardware firewalls, or both, depending on their structure.
- Each type of firewall has different functionality but the same purpose. However, it is best practice to have both to achieve maximum possible protection.
- A hardware firewall is a physical device that attaches between a computer network and a gateway.
- For example- a broadband router.
- A hardware firewall is sometimes referred to as an Appliance Firewall.
- On the other hand, a software firewall is a simple program installed on a computer that works through port numbers and other installed software. This type of firewall is also called a Host Firewall.

1. Packet Filtering Firewalls

- Packet filtering firewalls are the oldest, most basic type of firewalls.
- Operating at the network layer, they check a data packet for its source IP and destination IP, the protocol, source port, and destination port against predefined rules to determine whether to pass or discard the packet.
- Packet filtering firewalls are essentially stateless, monitoring each packet independently without any track of the established connection or the packets that have passed through that connection previously.
- This makes these firewalls very limited in their capacity to protect against advanced threats and attacks.
- Packet filtering firewalls are fast, cheap, and effective.
- But the security they provide is very basic.
- Since these firewalls cannot examine the content of the data packets, they are incapable of protecting against malicious data packets coming from trusted source IPs.
- Being stateless, they are also vulnerable to source routing attacks and tiny fragment attacks.
- But despite their minimal functionality, packet filtering firewalls paved the way for modern firewalls that offer stronger and deeper security.

2. Circuit-Level Gateways

- Working at the session layer, circuit-level gateways verify established Transmission Control Protocol (TCP) connections and keep track of the active sessions.
- They are quite similar to packet filtering firewalls in that they perform a single check and utilize minimal resources.
- However, they function at a higher layer of the Open Systems Interconnection (OSI) model.
- Primarily, they determine the security of an established connection.
- When an internal device initiates a connection with a remote host, circuit-level gateways establish a virtual connection on behalf of the internal device to keep the identity and IP address of the internal user hidden.
- Circuit-level gateways are cost-efficient, simplistic, barely impact a network's performance.
- However, their inability to inspect the content of data packets makes them an incomplete security solution on their own.
- A data packet containing malware can bypass a circuit-level gateway easily if it has a legitimate TCP handshake.
- That is why another type of firewall is often configured on top of circuit-level gateways for added protection.
- **3. Stateful Inspection Firewalls**
- A step ahead of circuit-level gateways, stateful inspection firewalls, and verifying and keeping track of established connections also perform packet inspection to provide better, more comprehensive security.
- They work by creating a state table with source IP, destination IP, source port, and destination port once a connection is established.
- They create their own rules dynamically to allow expected incoming network traffic instead of relying on a hardcoded set of rules based on this information.
- They conveniently drop data packets that do not belong to a verified active connection.
- Stateful inspection firewalls check for legitimate connections and source and destination IPs to determine which data packets can pass through.
- Although these extra checks provide advanced security, they consume a lot of system resources and can slow down traffic considerably.
- Hence, they are prone to DDoS (distributed denial-of-service attacks).
- **4. Application-Level Gateways (Proxy Firewalls)**
- Application-level gateways, also known as proxy firewalls, are implemented at the application layer via a proxy device.
- Instead of an outsider accessing your internal network directly, the connection is established through the proxy firewall.
- The external client sends a request to the proxy firewall.

- After verifying the authenticity of the request, the proxy firewall forwards it to one of the internal devices or servers on the client’s behalf.
- Alternatively, an internal device may request access to a webpage, and the proxy device will forward the request while hiding the identity and location of the internal devices and network.
- Unlike packet filtering firewalls, proxy firewalls perform stateful and deep packet inspection to analyze the context and content of data packets against a set of user-defined rules.
- Based on the outcome, they either permit or discard a packet.
- They protect the identity and location of your sensitive resources by preventing a direct connection between internal systems and external networks.
- However, configuring them to achieve optimal network protection can be tricky.
- You must also keep in mind the tradeoff—a proxy firewall is essentially an extra barrier between the host and the client, causing considerable slowdowns.

User Management

- User management is an organizational function that enables users to access and control digital assets, such as applications, devices, networks, and cloud services.
- Organizations are now exploring even more advanced solutions. Modern user management services provide end-to-end management of user accounts, including user registration, login and authentication, single sign-on (SSO), and permissions management.
- User management functions include:
    - Preventing unauthorized access to infrastructure, applications, and data
    - Storing user details and credentials
    - Providing a convenient login mechanism for end-users
    - Allowing users to set and reset passwords
    - Enabling multi-factor authentication (MFA)
    - Assigning user rights to systems, services, and applications
    - Managing user entitlements within services and applications

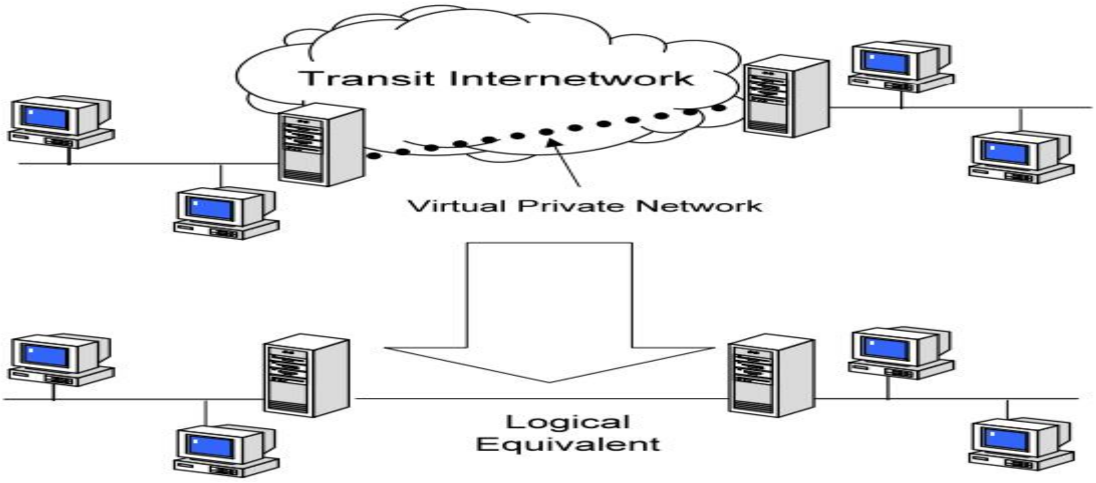
- A solution commonly used to implement user management is identity and access management (IAM).
- IAM enables administrators to define access to IT resources, both for internal and external users.
- IAM either includes or integrates with a user directory service, which contains credentials and other details of all users.
- The directory service enforces access controls by authenticating, authorizing, and auditing user access.

The Need for Modern User Management

- User management allows administrators to manage resources and organize users according to their needs and roles while maintaining the security of IT systems.
- Administrators need powerful user management capabilities that can allow them to group users and define flexible access policies.
- For end-users, many parts of user management are invisible.
- When users are exposed to user management—for example, when they use a login box to access an application—they expect the interaction to be simple and seamless.
- Login is a frequently-performed, critical operation, meaning that any delay or malfunction annoys users and hurts productivity.

VPN Security

- VPN stands for "Virtual Private Network" and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in real time.



Why should you use a VPN connection?

- Your ISP usually sets up your connection when you connect to the internet.
- It tracks you via an IP address.
- Your network traffic is routed through your ISP's servers, which can log and display everything you do online.
- Your ISP may seem trustworthy, but it may share your browsing history with advertisers, the police or government, and/or other third parties.

- ISPs can also fall victim to attacks by cyber criminals: If they are hacked, your personal and private data can be compromised.
- This is especially important if you regularly connect to public Wi-Fi networks.
- You never know who might be monitoring your internet traffic and what they might steal from you, including passwords, personal data, payment information, or even your entire identity.

What are the benefits of a VPN connection?

A VPN connection disguises your data traffic online and protects it from external access. Unencrypted data can be viewed by anyone who has network access and wants to see it. With a VPN, hackers and cyber criminals can't decipher this data.

- **Secure encryption:** To read the data, you need an *encryption key* . Without one, it would take millions of years for a computer to decipher the code in the event of a brute force attack . With the help of a VPN, your online activities are hidden even on public networks.
- **Disguising your whereabouts** : VPN servers essentially act as your proxies on the internet. Because the demographic location data comes from a server in another country, your actual location cannot be determined. In addition, most VPN services do not store logs of your activities. Some providers, on the other hand, record your behavior, but do not pass this information on to third parties. This means that any potential record of your user behavior remains permanently hidden.
- **Access to regional content:** Regional web content is not always accessible from everywhere. Services and websites often contain content that can only be accessed from certain parts of the world. Standard connections use local servers in the country to determine your location. This means that you cannot access content at home while traveling, and you cannot access international content from home. With **VPN location**
- **spoofing** , you can switch to a server to another country and effectively "change" your location.
- **Secure data transfer:** If you work remotely, you may need to access important files on your company's network. For security reasons, this kind of information requires a secure connection. To gain access to the network, a VPN connection is often required. VPN services connect to private servers and use encryption methods to reduce the risk of data leakage.

Security Protocols

- A protocol is a series of steps carried out by two or more entities. Ex: HTTP, TCP, SMTP
- A security protocol is a protocol that runs in an untrusted environment and tries to achieve a security goal.
- Academic examples / Industrial examples

Academic examples	Industrial examples
Needham-Schroeder-Lowe	Kerberos
Diffie Hellman key exchange	SSL/TLS PAKE IPSec

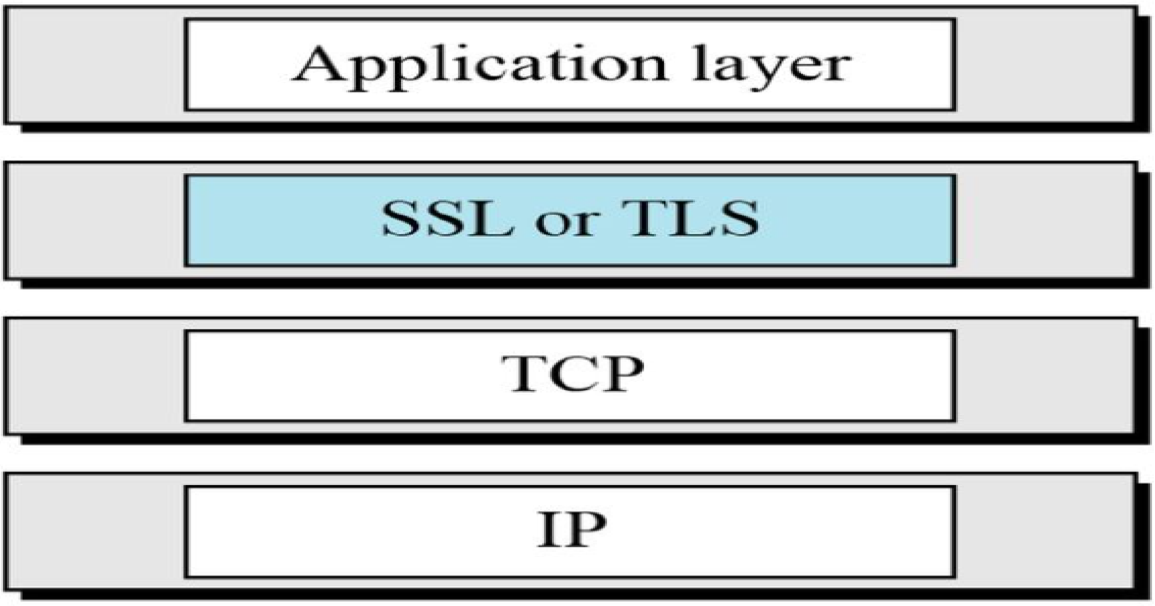
- Security protocols usually assume:

■ Untrusted channels: Hostile agents that do not participate in the protocol have access to the communication medium.

■ Dishonest participants: Hostile agents that claim to be honest, but try to prevent the security goals from being achieved.

Security at the transport layer SSL and TLS

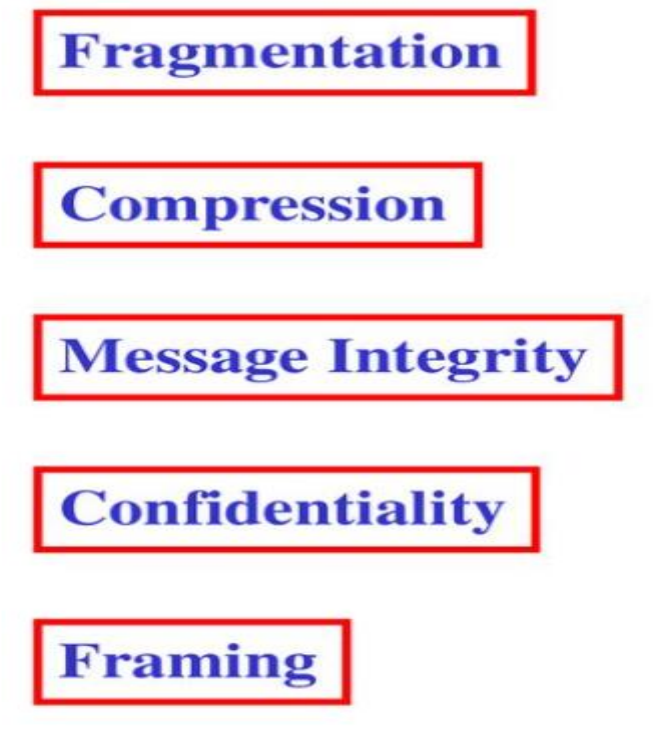
Location of SSL and TLS in the internet model



SSL Architecture

SSL is designed to provide security and compression services to data generated from the application layer.originally developed by Netscape.version 3 designed with public input. uses TCP to provide a reliable end-to-end service

Services Algorithms



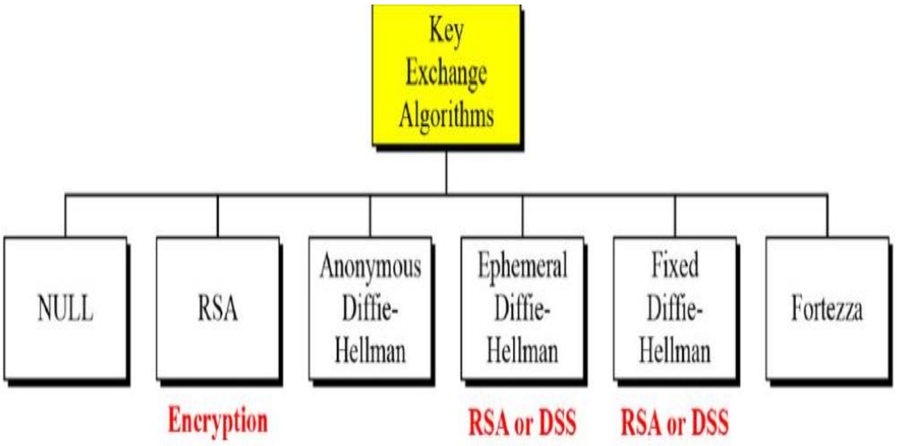
Fragmentation

Compression

Message Integrity

Confidentiality

Framing

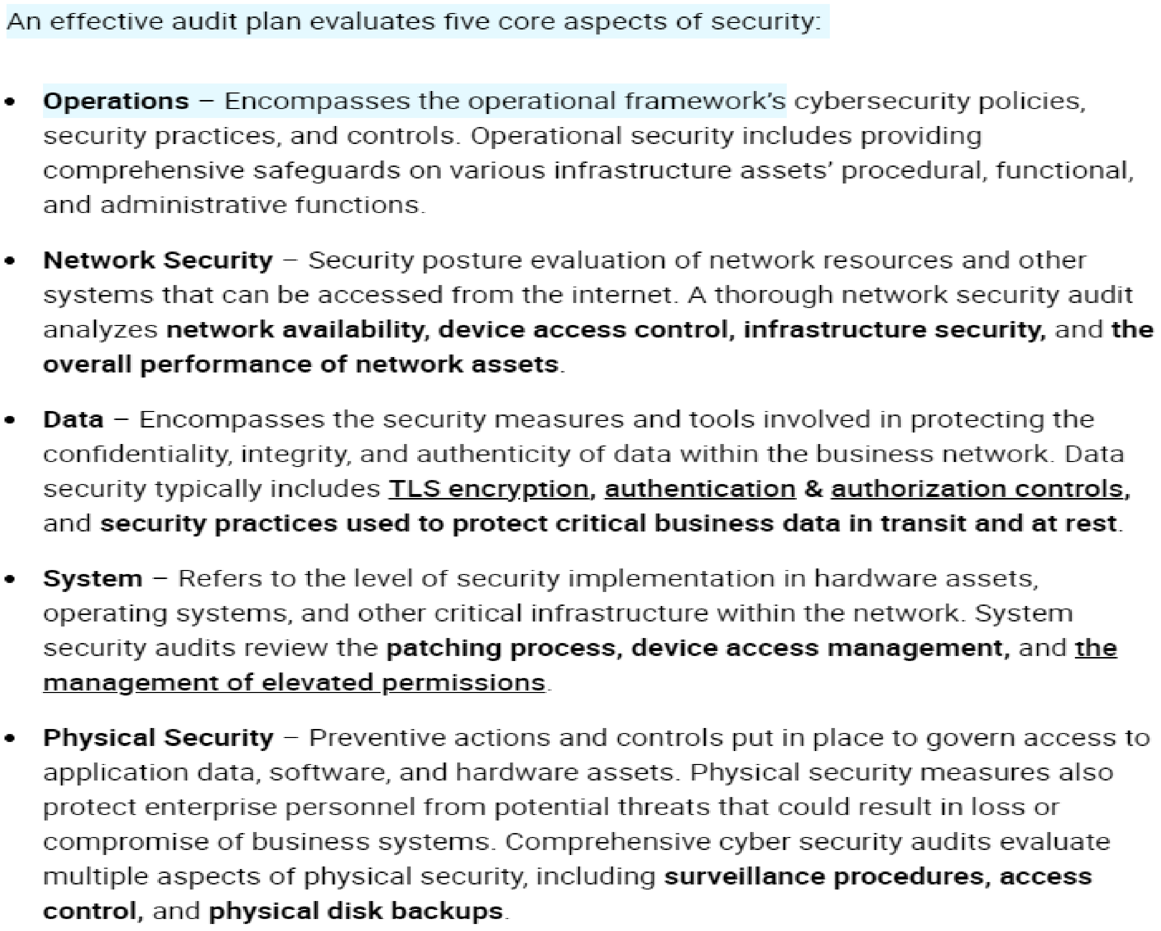


UNIT-4

Cybersecurity Audit and Standards

What is a Cybersecurity Audit?

A cybersecurity audit provides a comprehensive assessment of information systems to evaluate compliance and identify gaps in security policy implementation. The auditing process involves closely examining the firm's digital assets and security controls to ensure they satisfy compliance standards requirements. Besides offering insights into existing security vulnerabilities, a comprehensive audit also includes mitigation actions to mitigate cyber threats.



An effective audit plan evaluates five core aspects of security:

- **Operations** – Encompasses the operational framework's cybersecurity policies, security practices, and controls. Operational security includes providing comprehensive safeguards on various infrastructure assets' procedural, functional, and administrative functions.
- **Network Security** – Security posture evaluation of network resources and other systems that can be accessed from the internet. A thorough network security audit analyzes **network availability, device access control, infrastructure security,** and **the overall performance of network assets**.
- **Data** – Encompasses the security measures and tools involved in protecting the confidentiality, integrity, and authenticity of data within the business network. Data security typically includes **TLS encryption**, **authentication** & **authorization controls**, and **security practices used to protect critical business data in transit and at rest**.
- **System** – Refers to the level of security implementation in hardware assets, operating systems, and other critical infrastructure within the network. System security audits review the **patching process, device access management,** and **the management of elevated permissions**.
- **Physical Security** – Preventive actions and controls put in place to govern access to application data, software, and hardware assets. Physical security measures also protect enterprise personnel from potential threats that could result in loss or compromise of business systems. Comprehensive cyber security audits evaluate multiple aspects of physical security, including **surveillance procedures, access control,** and **physical disk backups**.

Satisfying compliance regulations

All enterprise systems that process information are guided by security compliance frameworks and governance institutes, such as the **National Institute of Standards and Technology (NIST)**, **Health Insurance Portability and Accountability Act (HIPAA)**, and **Control Objectives for Information and Related Technology (COIRT)**. Such frameworks outline compliance audits as a statutory requirement, which help reduces the company's legal risk. Compliance audits determine whether the organization adheres to these frameworks' policies, rules, and guidelines.

Enforces business continuity

A comprehensive cybersecurity audit helps identify security gaps that can be exploited to orchestrate attacks and document possible mitigations for an exploit. Security professionals and operators rely on audit analytics to administer appropriate security mechanisms for regaining control of key infrastructure already compromised by malicious actors. A security audit includes backup and disaster recovery plans to ensure business systems are available during a security breach. The process ensures minimal business disruptions even in an active attack.

Improves reputational value

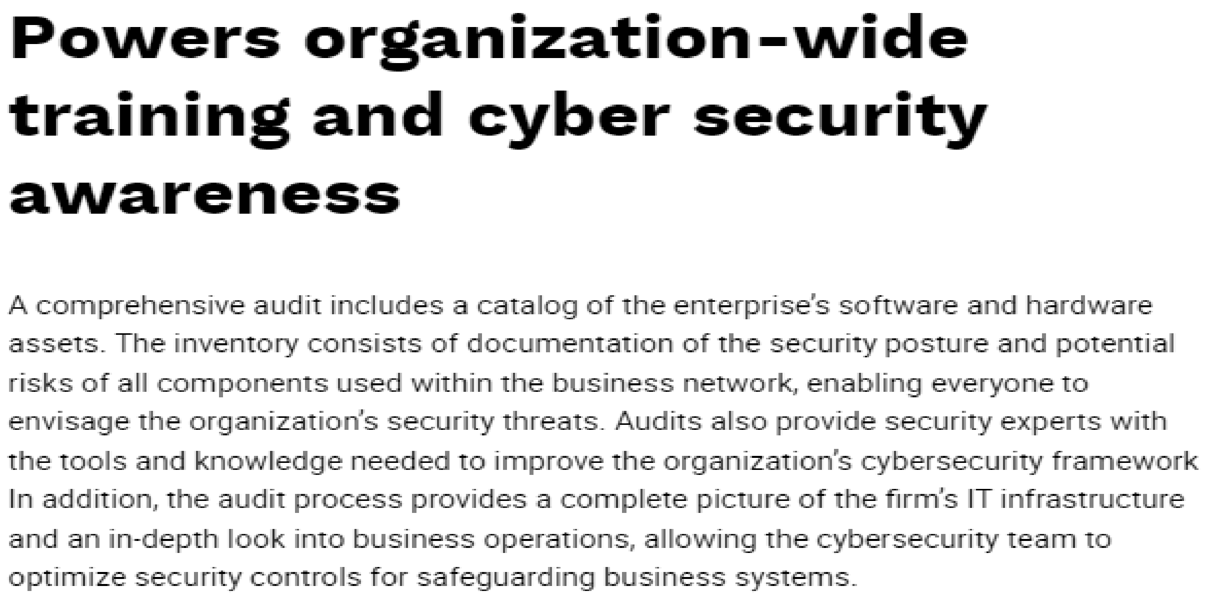
Cybersecurity issues damage an organization's reputation since users avoid trusting a company if it can't secure its digital assets. When attackers obtain user accounts or organizational data, they can access sensitive information and key infrastructure, leading to data breaches, application availability, and intellectual property theft. Through regular audits, organizations can proactively identify and fix cybersecurity threats in the business network, earning public trust. Compliance audits also evaluate how the firm adheres to regulatory requirements and security standards, featuring the company's performance within its industry.

Benefits of Cybersecurity Audits

An effective cybersecurity audit program helps evaluate and improve the security of enterprise systems, networks, connected devices, and underlying data. Some benefits of performing a comprehensive audit process include:

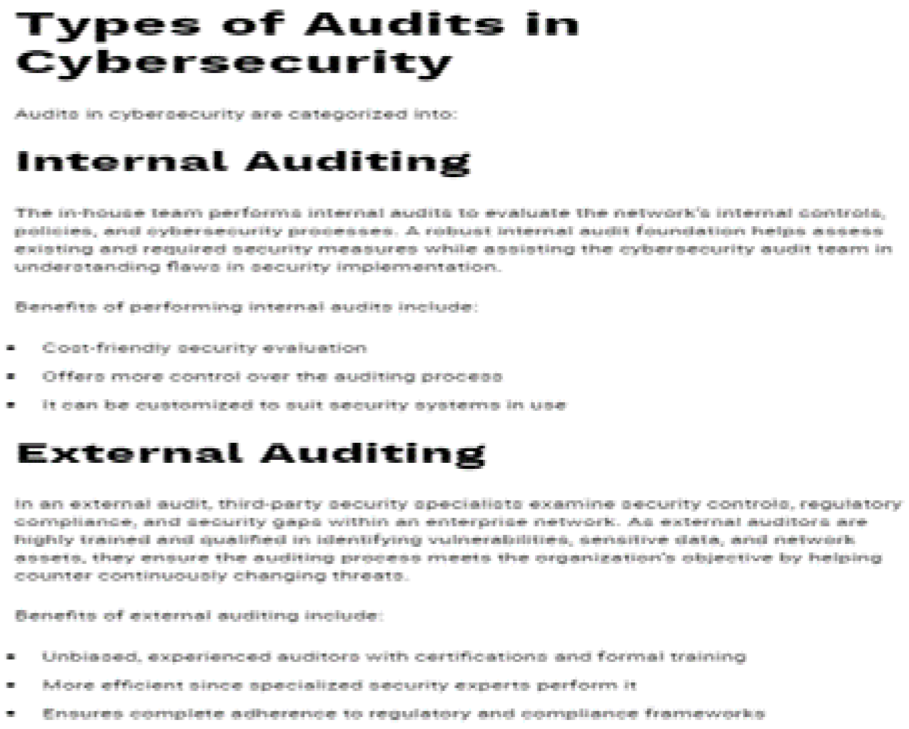
Helps to identify gaps in security

During a cybersecurity audit, security experts probe business systems for potential risks that can lead to breaches and business disruptions. The auditing process includes continuously monitoring the entire business network to detect and identify flaws that can be exploited for an attack. Exposing weaknesses and high-risk policies helps security analysts create risk management plans and improvise an existing cybersecurity strategy.



Powers organization-wide training and cyber security awareness

A comprehensive audit includes a catalog of the enterprise's software and hardware assets. The inventory consists of documentation of the security posture and potential risks of all components used within the business network, enabling everyone to envisage the organization's security threats. Audits also provide security experts with the tools and knowledge needed to improve the organization's cybersecurity framework In addition, the audit process provides a complete picture of the firm's IT infrastructure and an in-depth look into business operations, allowing the cybersecurity team to optimize security controls for safeguarding business systems.



Types of Audits in Cybersecurity

Audits in cybersecurity are categorized into:

Internal Auditing

The in-house team performs internal audits to evaluate the network's internal controls, policies, and cybersecurity processes. A robust internal audit foundation helps assess existing and required security measures while assisting the cybersecurity audit team in understanding flaws in security implementation.

Benefits of performing internal audits include:

- Cost-friendly security evaluation
- Offers more control over the auditing process
- It can be customized to suit security systems in use

External Auditing

In an external audit, third-party security specialists examine security controls, regulatory compliance, and security gaps within an enterprise network. As external auditors are highly trained and qualified in identifying vulnerabilities, sensitive data, and network assets, they ensure the auditing process meets the organization's objective by helping counter continuously changing threats.

Benefits of external auditing include:

- Unbiased, experienced auditors with certifications and formal training
- More efficient since specialized security experts perform it
- Ensures complete adherence to regulatory and compliance frameworks

Cybersecurity standards

Cybersecurity standards are techniques generally set forth in published materials that attempt to protect the cyber environment of a user or organization.

This environment includes:

users themselves

networks

devices

all software

processes

information in storage or transit

applications

services

systems that can be connected directly or indirectly to networks

The principal objective:

to reduce the risks

including prevention or mitigation of cyber-attacks.

Cybersecurity standards have existed over several decades as users and providers have collaborated in many domestic and international forums to effect the necessary capabilities, policies, and practices - generally emerging from work at the Stanford Consortium for Research on Information Security and Policy in the 1990s.

Also many tasks that were once carried out by hand are now carried out by computer; therefore there is a need for information assurance (IA) and security.

Around 70% of the surveyed organizations see the NIST Cybersecurity Framework as the most popular best practice for computer security, but many note that it requires significant investment (US SFA study report, 2016)

NIST Cybersecurity Framework (NIST CSF)

The NIST Cybersecurity Framework (NIST CSF) provides a policy framework of computer security guidance for how private sector organizations in the US can assess and improve their ability to prevent, detect, and respond to cyber attacks.

It provides a high level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes.

It is intended to help private sector organizations that provide critical infrastructure with guidance on how to protect it, along with relevant protections for privacy and civil liberties.

ETSI Cyber Security Technical Committee (TC CYBER)

TC CYBER is responsible for the standardization of Cyber Security internationally and for providing a center of relevant expertise for other ETSI committees(**European Telecommunications Standards Institute)**.

Growing dependence on networked digital systems has brought with it an increase in both the variety and quantity of cyber-threats.

The different methods governing secure transactions in the various Member States of the EU sometimes make it difficult to assess the respective risks and to ensure adequate security.

Building on ETSI's world-leading expertise in the security of Information and Communications Technologies (ICT), it set up a new Cyber Security committee (TC CYBER) in 2014 to meet the growing demand for standards to protect the Internet and the communications and business it carries.

ISO/IEC and 27002

SO/IEC 27001, part of the growing ISO/IEC family of standards, is an information security management system (ISMS) standard, of which the last revision was published in October 2013 by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC).

Its full name is ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements.

ISO/IEC formally specifies a management system that is intended to bring information security under explicit management control.

CISQ-Consortium for IT Software Quality

CISQ develops standards for automating the measurement of software size and software structural quality.

CISQ is a special interest group of the Object Management Group that submits specifications for approval as OMG international standards.

The measurement standards are used for the static program analysis of software, a software testing practice that identifies critical vulnerabilities in the code and architecture of a software system.

CISQ-developed standards are used to manage the Security, Reliability, Performance Efficiency and Maintainability characteristics of software risk.

COBIT

COBIT was developed in the mid-1990s by ISACA, an independent organization of IT governance professionals. ISACA offers the well-known Certified Information Systems Auditor and Certified Information Security Manager certifications.COBIT originally focused on reducing IT risks. COBIT 5, released in 2012, included new technology and business trends to help organizations balance IT and business goals. The current version is COBIT 2019. It's the most used framework to achieve Sarbanes-Oxley compliance. Numerous publications and professional certifications address COBIT requirements.

Risk Assessment and Management

What is a cyber security risk assessment?

- A cyber security risk assessment is the process of identifying, analysing and evaluating risk. It helps to ensure that the cyber security controls you choose are appropriate to the risks your organisation faces.
- Without a risk assessment to inform your cyber security choices, you could waste time, effort and resources. There is little point implementing measures to defend against events that are unlikely to occur or won't impact your organisation.
- Likewise, you might underestimate or overlook risks that could cause significant damage. This is why so many best-practice frameworks, standards and laws – including the GDPR (General Data Protection Regulation) – require risk assessments to be conducted.

How do you conduct a cyber security risk assessment?

- A cyber security risk assessment identifies the information assets that could be affected by a cyber attack (such as hardware, systems, laptops, customer data and intellectual property). It then identifies the risks that could affect those assets.
- A risk estimation and evaluation are usually performed, followed by the selection of controls to treat the identified risks.
- It is essential to continually monitor and review the risk environment to detect any changes in the context of the organisation, and to maintain an overview of the complete risk management process

What does a cyber security risk assessment include?

- A typical risk assessment involves identifying the various information assets that could be affected by a cyber attack (such as hardware, systems, laptops, customer data, intellectual property, etc.), followed by identifying the various risks that could affect those assets.
- A risk estimation and evaluation is usually performed, followed by the selection of controls necessary to treat the identified risks.
- It is important to continually monitor and review the risk environment to detect any changes in the context of the organisation, and to maintain an overview of the complete risk management process.

ISO 27001 and cyber risks

- The international standard ISO/IEC 27001:2013 (ISO 27001) provides the specifications for a best-practice ISMS (information security management system) – a risk-based approach to information security risk management that addresses people, processes and technology.
- Clause 6.1.2 of the Standard sets out the requirements of the information security risk assessment process. Organisations must:

1. Establish and maintain specific information security risk criteria;
2. Ensure that repeated risk assessments "produce consistent, valid and comparable results";
3. Identify "risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system" and identify the owners of those risks; and
4. Analyse and evaluate information security risks, according to the criteria established earlier.
5. It is essential that organisations "retain documented information about the information security risk assessment process" so that they can demonstrate that they comply with these requirements.

They will also need to follow several steps – and create relevant documentation – as part of the information security risk treatment process

IT Governance cyber risk assessment service

- Our team of qualified cyber security advisers will provide business-driven consultation on the overall process of assessing information risk. They will offer support, guidance and advice in the following areas:

1. Identifying the assets that require protection.
2. Identifying relevant threats and weaknesses.
3. Identifying exploitable vulnerabilities.
4. Assessing the level of threat posed by threat agents.
5. Determining the business impacts of risks being realised.
6. Producing a security risk assessment.
7. Advising on a risk acceptance threshold or level of acceptance.
8. Advising on suitable control implementation.

Cyber risk assessment should be a continual activity. A comprehensive enterprise security risk assessment should be conducted at least once a year or when significant changes occur to the business, the IT estate, or legal environment to explore the risks associated with the organisation's information systems. An enterprise security risk assessment can only give a snapshot of the risks of the information systems at a particular point in time.

Asset Classification

All the Company's information, data and communication must be classified strictly according to its level of confidentiality, sensitivity, value and criticality. Information may be classified as HIGHLY RESTRICTED, CONFIDENTIAL, INTERNAL USE ONLY, and PUBLIC.

HIGHLY RESTRICTED: This classification label applies to the most private or otherwise sensitive information of the Company. Information under this classification shall be strictly monitored and controlled at all times. (e.g. merger and acquisition documents, corporate level strategic plans, litigation strategy memos, reports on breakthrough new product research, and Trade Secrets such as certain computer programs

CONFIDENTIAL: This classification label applies to Company information, which is private or otherwise sensitive in nature and shall be restricted to those with a legitimate business need for access. (e.g. employee performance evaluations, customer transaction data, strategic alliance agreements, unpublished internally generated market research, computer passwords, identity token personal identification numbers (PINs), and internal audit reports.

INTERNAL USE ONLY: This classification label applies to information intended for use within the Company, and in some cases within affiliated organizations, such as business partners of the Company. Assets of this type are widely-distributed within the Company and may be distributed within Company without permission from the information asset owner. (e.g. telephone directory, dial-up computer access numbers, new employee training materials, and internal policy manuals.

PUBLIC: This classification applies to information that has been explicitly approved by the Company's management for release to the public. Assets of this type may be circulated without potential harm. (e.g. prod

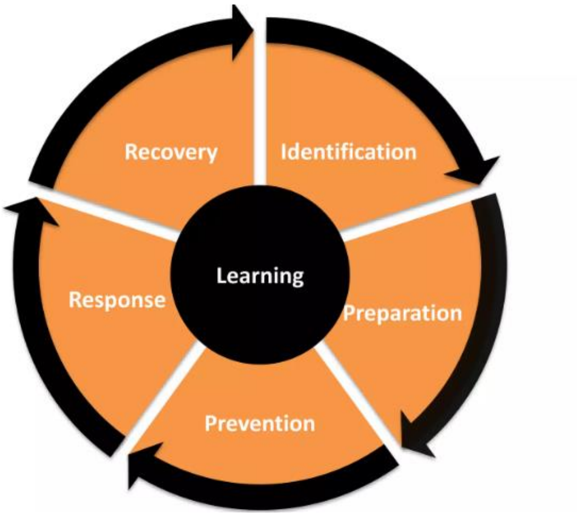
Crisis Management Plan

The word crisis comes from two Chinese words; Danger and Opportunity.

Crisis: is any event that is expected to lead to, an unstable and dangerous situation affecting an individual, group, or whole organization.

Crisis Management: is the process by which an organization deals with a major event that threatens to harm the organization, its stakeholders, or the general public.

Crisis Management Cycle



First Stage of crisis management is

IDENTIFYING the crisis' nature.

• Crisis can be clustered into:

– Natural crisis: occur due to natural disasters.

– Organizational Misdeed crisis: occur when management take actions that harm stakeholders without suitable precautions.

– Deception crisis: occur due to lack of transparency from the management about certain information.

– Workplace violence crisis: occur when member commit violence to other members.

– Skewed values crisis: occur when short- term gain is favored and values are neglected.

– Rumors crisis: occur when false information about an organization and its product hurt the organization's reputation.

Second Stage is PREPARING for the crisis.

• Crisis preparation is done by:

– Vulnerability Assessment: determine current and potential areas of operational and communications weakness.

– Crisis Planning: are two types

• Operational : What we do, who does it, and when it is done.

• Communications: what do we say, who says it, how do we get the messages out. Preparation

Third stage is PREVENTING the crisis from happening.

• Crisis Prevention is occurred by:

– Anticipate and Have a plan.

– Respond immediately.

– Do not over talk.

– Always tell the truth.

– Accept responsibility. Prevention

Fourth stage is RESPONDING to the crisis. • Effective crisis response includes: – Set of planning scenarios. – Set of response modules. – Preset activation protocols. – Clear communication channels. Response

Fifth stage is RECOVERING from the crisis. • Organizations must be able to carry on with their business in the middle of the crisis. • while simultaneously planning for how they will recover from the damage the crisis caused. • Crisis handlers must engage in the recovery plan while perusing the goal. Recovery