**Information Security Areas**

## 1. Information security and Availability, Integrity and Confidentiality (AIC) traid

**Confidentiality, integrity and availability**, also known as the **CIA triad**, is a model designed to guide policies for information security within an organization. The model is also sometimes referred to as the AIC triad (availability, integrity andconfidentiality) to avoid confusion with the Central Intelligence Agency. The elements of the triad are considered the three most crucial components of security.

In this context, confidentiality is a set of rules thatlimits access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of reliable access to the information by authorized people.

**Confidentiality:**

Confidentiality is roughly equivalent to privacy. Measures undertaken to ensure confidentiality aredesigned to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it: Access must be restricted to those authorized to view the data in question. It is common, as well, for data to be categorized according to the amount and type of damage that could be done should it fall into unintended hands. More or less stringent measures can then be implemented according to those categories.

Sometimes safeguarding data confidentiality may involve special training for those privy to such documents. Such training would typically include security risks that could threaten this information. Training can help familiarize authorized people with risk factors and how to guard against them. Further aspects of training can include strong passwords and password-related best practices and information about social engineering methods, to prevent them from bending data-handling rules with good intentions and potentially disastrous results.

A good example of methods used to ensure confidentiality is an account number or routing number when banking online. Data encryption is a common method of ensuring confidentiality. User IDs and passwords constitute a standard procedure; two-factor authentication is becoming the norm. Other options include biometric verification and security tokens, key fobs or soft tokens. In addition, users can take precautions to minimize the number of places where the information appears and the number of times it is actually transmitted to complete a required transaction. Extra measures might be taken in the case of extremely sensitive documents, precautions such as storing only on air gapped computers, disconnected storage devices or, for highly sensitive information, in hard copy form only.

**Integrity:**

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality). These measures include file permissions and user access controls. Version control maybe used to prevent erroneous changes or accidental deletion by authorized users becoming a problem. In addition, some means must be in place to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse (EMP) or server crash. Some data might include checksums, even cryptographic checksums, for verification of integrity. Backups or redundancies must be available to restore the affected data to its correct state.

**Availability:**

Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts. It's also important to keep current with all necessary system upgrades. Providing adequate communication bandwidth and preventing the occurrence of bottlenecks are equally important. Redundancy, failover, RAID even high-availability clusters can mitigate serious consequences when hardware issues do occur. Fast and adaptive disaster recovery is essential for the worst case scenarios; that capacity is reliant on the existence of a comprehensive disaster recovery plan (DRP). Safeguards against data loss or interruptions in connections must include unpredictable events such as natural disasters and fire. To prevent data loss from such occurrences, a backup copy may be stored in a geographically-isolated location, perhaps even in a fireproof, waterproof safe. Extra security equipment or software such as firewalls and proxy servers can guard against downtime and unreachable data due to malicious actions such as denial-of-service (DoS) attacks and network intrusions.

## 2. Characteristics of Information

Good information is that which is used and which creates value. Experience and research shows that good information has numerous qualities.

Good information is relevant for its purpose, sufficiently accurate for its purpose, complete enough for the problem, reliable and targeted to the right person. It is also communicated in time for its purpose, contains the right level of detail and is communicated by an appropriate channel, i.e. one that is understandable to the user.

Further details of these characteristics related to organisational information for decision-making follows.

**Availability/accessibility**

Information should be easy to obtain or access. Information kept in a book of some kind is only available and easy to access if you have the book to hand. A good example of availability is a telephone directory, as every home has one for its local area. It is

probably the first place you look for a local number. But nobody keeps the whole country's telephone books so for numbers further afield you probably phone a directory enquiry number. For business premises, say for a hotel in London, you would probably use the Internet.

Businesses used to keep customer details on a card-index system at the customer's branch. If the customer visited a different branch a telephone call would be needed to check details. Now, with centralised computer systems, businesses like banks and building societies can access any customer's data from any branch.

**Accuracy**

Information needs to be accurate enough for the use to which it is going to be put. To obtain information that is 100% accurate is usually unrealistic as it is likely to be too expensive to produce on time. The degree of accuracy depends upon the circumstances. At operational levels information may need to be accurate to the nearest penny – on a supermarket till receipt, for example. At tactical level department heads may see weekly summaries correct to the nearest £100, whereas at strategic level directors may look at comparing stores' performances over several months to the nearest £100,000 per month.

Accuracy is important. As an example, if government statistics based on the last census wrongly show an increase in births within an area, plans may be made to build schools and construction companies may invest in new housing developments. In these cases any investment may not be recouped.

**Reliability or objectivity**

Reliability deals with the truth of information or the objectivity with which it is presented. You can only really use information confidently if you are sure of its reliability and objectivity.

When researching for an essay in any subject, we might make straight for the library to find a suitable book. We are reasonably confident that the information found in a book, especially one that the library has purchased, is reliable and (in the case of factual information) objective. The book has been written and the author's name is usually printed for all to see. The publisher should have employed an editor and an expert in the field to edit the book and question any factual doubts they may have. In short, much time and energy goes into publishing a book and for that reason we can be reasonably confident that the information is reliable and objective.

Compare that to finding information on the Internet where anybody can write unedited and unverified material and 'publish' it on the web. Unless you know who the author is, or a reputable university or government agency backs up the research, then you cannot be sure that the information is reliable. Some Internet websites are like vanity publishing, where anyone can write a book and pay certain (vanity) publishers to publish it.

**Relevance/appropriateness**

Information should be relevant to the purpose for which it is required. It must be suitable. What is relevant for one manager may not be relevant for another. The user will become frustrated if information contains data irrelevant to the task in hand.

For example, a market research company may give information on users' perceptions of the quality of a product. This is not relevant for the manager who wants to know opinions on relative prices of the product and its rivals. The information gained would not be relevant to the purpose.

**Completeness**

Information should contain all the details required by the user. Otherwise, it may not be useful as the basis for making a decision. For example, if an organisation is supplied with information regarding the costs of supplying a fleet of cars for the sales force, and servicing and maintenance costs are not included, then a costing based on the information supplied will be considerably underestimated.

Ideally all the information needed for a particular decision should be available. However, this rarely happens; good information is often incomplete. To meet all the needs of the situation, you often have to collect it from a variety of sources.

**Level of detail/conciseness**

Information should be in a form that is short enough to allow for its examination and use. There should be no extraneous information. For example, it is very common practice to summarise financial data and present this information, both in the form of figures and by using a chart or graph. We would say that the graph is more concise than the tables of figures as there is little or no extraneous information in the graph or chart. Clearly there is a trade-off between level of detail and conciseness.

**Presentation**

The presentation of information is important to the user. Information can be more easily assimilated if it is aesthetically pleasing. For example, a marketing report that includes graphs of statistics will be more concise as well as more aesthetically pleasing to the users within the organisation. Many organisations use presentation software and show summary information via a data projector. These presentations have usually been well thought out to be visually attractive and to convey the correct amount of detail.

**Timing**

Information must be on time for the purpose for which it is required. Information received too late will be irrelevant. For example, if you receive a brochure from a theatre and notice there was a concert by your favourite band yesterday, then the information is too late to be of use.

**Value of information**

The relative importance of information for decision-making can increase or decrease its value to an organisation. For example, an organisation requires information on a competitor's performance that is critical to their own decision on whether to invest in new machinery for their factory. The value of this information would be high. Always keep in mind that information should be available on time, within cost constraints and be legally obtained.

**Cost of information**

Information should be available within set cost levels that may vary dependent on situation. If costs are too high to obtain information an organisation may decide to seek slightly less comprehensive information elsewhere. For example, an organisation wants to commission a market survey on a new product. The survey could cost more than the forecast initial profit from the product. In that situation, the organisation would probably decide that a less costly source of information should be used, even if it may give inferior information.

**The difference between value and cost**

Many students in the past few years have confused the definitions of value and cost. Information gained or used by an organisation may have a great deal of value even if it may not have cost a lot. An example would be bookshops, who have used technology for many years now, with microfiche giving way to computers in the mid to late 1990s. Microfiche was quite expensive and what the bookshops received was essentially a list of books in print. By searching their microfiche by publisher they could tell you if a particular book was in print. Eventually this information became available on CD-ROM. Obviously this information has value to the bookshops in that they can tell you whether or not you can get the book. The cost of subscribing to microfiche was fairly high; subscribing to the CD-ROM version only slightly less so.

Much more valuable is a stock system which can tell you instantly whether or not the book is in stock, linked to an on-line system which can tell you if the book exists, where it is available from, the cost and delivery time. This information has far more value than the other two systems, but probably actually costs quite a bit less. It is always up-to-date and stock levels are accurate.

## 3. Threats to information security

Modern technology and society's constant connection to the Internet allows more creativity in business than ever before – including the black market. Cybercriminals are carefully discovering new ways to tap the most sensitive networks in the world. Protecting business data is a growing challenge but awareness is the first step. Here are the top 10 threats to information security today:

**Technology with Weak Security** – New technology is being released every day. More times than not, new gadgets have some form of Internet access but no plan for security. This presents a very serious risk – each unsecured connection means vulnerability. The rapid development of technology is a testament to innovators, however security lags severely[1].

**Social Media Attacks** – Cybercriminals are leveraging social media as a medium to distribute a complex geographical attack called "water holing". The attackers identify and infect a cluster of websites they believe members of the targeted organization will visit[2].

**Mobile Malware** – Security experts have seen risk in mobile device security since the early stages of their connectivity to the Internet. The minimal mobile foul play among the long list of recent attacks has users far less concerned than they should be. Considering our culture's unbreakable reliance on cell phones and how little cybercriminals have targeted them, it creates a catastrophic threat.

**Third-party Entry** – Cybercriminals prefer the path of least resistance. Target is the poster child of a major network attack through third-party entry points. The global retailer's HVAC vendor was the unfortunate contractor whose credentials were stolen and used to steal financial data sets for 70 million customers[3].

**Neglecting Proper Configuration** – Big data tools come with the ability to be customized to fit an organization's needs. Companies continue to neglect the importance of properly configuring security settings. The New York Times recently fell victim to a data breach as a result of enabling only one of the several critical functionalities needed to fully protect the organization's information[4].

**Outdated Security Software** – Updating security software is a basic technology management practice and a mandatory step to protecting big data. Software is developed to defend against known threats. That means any new malicious code that hits an outdated version of security software will go undetected.

**Social Engineering** – Cybercriminals know intrusion techniques have a shelf life. They have turned to reliable non-technical methods like social engineering, which rely on social interaction and psychological manipulation to gain access to confidential data. This form of intrusion is unpredictable and effective.

**Lack of Encryption** – Protecting sensitive business data in transit and at rest is a measure few industries have yet to embrace, despite its effectiveness. The health care industry handles extremely sensitive data and understands the gravity of losing it – which is why HIPAA compliance requires every computer to be encrypted.

**Corporate Data on Personal Devices** – Whether an organization distributes corporate phones or not, confidential data is still being accessed on personal devices. Mobile management tools exist to limit functionality but securing the loopholes has not made it to the priority list for many organizations.

**Inadequate Security Technology** – Investing in software that monitors the security of a network has become a growing trend in the enterprise space after 2014's painful rip of data breaches. The software is designed to send alerts when intrusion attempts occur, however the alerts are only valuable if someone is available to address them. Companies are relying too heavily on technology to fully protect against attack when it is meant to be a managed tool.

## 4. Malicious Code and its attack types

Types of malicious code

- **Viruses**: pieces of code that attach to host programs and propagate when an infected program executes
  - **Memory-Resident Virus**
    This type will reside in main system memory. Whenever the operating system executes a file, the virus will infect a file if it is a suitable target, for example, a program file.
  - **Program File Virus**
    This will infect programs like EXE, COM, SYS etc.
  - **Polymorphic Virus**
    The virus itself can change form using various polymorphism techniques.
  - **Boot Sector Virus**
    This type will infect the system area of a disk, when the disk is accessed initially or booted.
  - **Stealth Virus**
    A virus which uses various stealth techniques in order to hide itself from detection by anti-virus software.
  - **Macro Virus**
    Unlike other virus types, these viruses attack data files instead of executable files.
    Macro viruses are particularly common due to the fact that:
    They attach to documents and files, which are platform independent.
    The document is sent to other computers by, for example, email or file exchange. Recipients are receiving the infected document from a "trusted" sender.
  - **Email virus**
    A virus spread by email messages.
- **Worms**: particular to networked computers, carry out pre-programmed attacks to jump across the network

One typical example of a massive attack is the "SQL Sapphire Slammer (Sapphire)" that occurred on 25 January 2003. The Sapphire exploited an MS SQL Server or MSDE 2000 database engine vulnerability. The weakness lays in an underlying indexing service that Microsoft had released a patch in 2002. It doubled in size every 8.5 seconds, and infected more than 90 percent of vulnerable hosts within 10 minutes. It eventually infected at least 75,000 hosts and caused network outages that resulted in:

- Canceled airline flights
- Interference with elections
- Bank ATM failures

- **Trojan Horses**: hide malicious intent inside a host program that appears to do something useful.

Some recent examples are:

- Trojan horses embedded into online game plug-ins which will help online gamer to advance their game characters; however, the online game account and password are also stolen. The gamer's cyber assets are therefore stolen.
- Trojan horses are embedded into popular commercial packages and uploaded to websites for free download or to be shared across peer-to-peer download networks.

### Spyware & Adware

Spyware is a type of software that secretly forwards information about a user to third parties without the user's knowledge or consent. This information can include a user's online activities, files accessed on the computer, or even user's keystrokes.
Adware is a type of software that displays advertising banners while a program is running. Some adware can also be spyware. They first spy on and gather information from a victim's computer, and then display an advertising banner related to the information collected.
A system with spyware / adware installed may display one or more of the following symptoms:

- The default start page of the web browser is changed to another website and/or new items are added to the Favorites folder without the user's consent. The user cannot undo the changes, and these browser hijackers force the user to visit the unwanted websites in order to, for example, inflate the hit rate of the websites for higher advertising value.
- Pop-up windows with advertisements open on the screen even when the user's browser is not running or when the system is not connected to the Internet.
- New software components, such as browser toolbars, are installed on a user's computer without his or her permission.
- Suspicious network traffic appears on the user's computer when he or she is not performing any online activities.

However, there are some spyware carefully programmed to avoid being noticed, and hence cannot be picked up by the above abnormalities. This type of spyware can only be detected and removed by anti-spyware products / tools.

**Tips for Prevention**

Besides the following common best practices, you should:

- Not download / install software from suspicious sources such as websites, peer-to-peer file sharing sources, etc.
- Read the terms and conditions of use, even before downloading and installing a legitimate piece of software, because they may require you to accept that an adware or spyware system be installed.
- Read the terms of use carefully when you are asked to install a plug-in or use active content when visiting some websites.
- Review the information provided by certain search engines whose search results may contain malicious code. This may help in avoiding dangerous or untrustworthy websites via search links.
- Install browser toolbars that can help filter out adware and spyware.
- Install anti-spyware and anti-adware software.

### Rootkit

A rootkit is a collection of files that alter the standard functionality of an operating system on a computer in a malicious and stealthy manner. By altering the operating system, a rootkit allows an attacker to act as system administer on the victim's system. (Or the "root" user in a Unix system - hence the name "rootkit".)

Many rootkits are designed to hide their existence and the changes they made to a system. This makes it very difficult to determine whether a rootkit is present on a system, and identify what has been changed by the rootkit. For example, a rootkit might suppress directory and process listing entries related to its own files.

Rootkits may be used to install other types of attacker tools, such as backdoors and keystroke loggers. Examples of rootkits include LRK5, Knark, Adore, and Hacker Defender.

### Active Content

Unlike the traditional methods of working with static data files using a software program, today's data objects, such as web pages, email and documents can interweave data and code together, allowing dynamic execution of program code on the user's computer. The fact that these data objects are frequently transferred between users makes them efficient carriers of viruses. The transparency of code execution can be a security concern.

The two main 'active content' technologies are ActiveX controls and Java. In general, ActiveX poses a greater threat because it has direct access to native Windows calls, and hence any system function. Java, on the other hand, is "sandboxed" or insulated from operating system services by the Java Virtual Machine. However, this does not mean that there will never be a Java virus.

### Tips for Prevention

Besides the following common best practices, you should:

- Watch out for any abnormal machine behaviour:
    - Programs taking much longer than usual to execute.
    - A sudden reduction in system memory, or available or disk space.
    - The browser home page was changed.
    - Some websites cannot be accessed anymore.
- Not install any active content from suspicious websites. Instead of selecting the decline option at the installation page, you should close the browser. This is because some installation pages may be a visual spoof, installing active content no matter which option is chosen. If it is not successful, you may consider using the task manager to force quit the browser.

### Zombies and Botnets

A zombie computer, usually known in the short form zombie, is a computer attached to the Internet that has been compromised and manipulated without the knowledge of the computer owner. A botnet refers to a network of zombie computers that have been taken over and put under the remote control of an attacker.

A botnet might consist of thousands of zombie computers, and even more. The zombie computers in the botnets can consist of computers at homes, schools, businesses and governments scattered around the world.

A zombie computer itself may only be slowed down slightly, or displaying mysterious messages. However, the whole botnet can be used by the attacker for a massive attack, such as DDoS (the Distributed Denial of Service) attack, against another system or network. Due to the large number of machines in a botnet, the aggregate computing power can be enormous when all these machines work together to launch a DDoS attack against a single target.

You should protect your machines or systems from becoming zombie computers.

### Scareware

Scareware, or sometimes called rogueware, comprises several classes of ransomware or scam software with malicious payloads. While pretending as legitimate anti-virus software or the likes, scareware is in fact dummy software without functions, or sometimes even a malicious software which may, for example, steal the victim's personal information and credentials such as passwords or credit card details. Ransomware makes your computer files inaccessible. The victim is then requested to pay a fee ("ransom") to regain access to their files.

Scareware usually entices victims by convincing them that a virus has infected their computer, then suggesting that they download (and pay for) an anti-virus software to remove it. Very often, the virus is entirely fictional, and the software installed is the

scareware itself. In additional to the loss of money paid for the scareware, the personal details and credit card information provided by the victim during the purchase of the scareware can be used by criminals in further fraud or sold on black market forums.
Ransomware is a twisted form of scareware. One of common tactics is that the malware attacks victims through phishing emails with a malicious attachment. Once infected, the malware makers of ransomware can "kidnap" user's computer and hold it to ransom by, for example, stopping the computer working, encrypting key system files or locking up some of the personal information. The victim needs to pay ransom to free their machines and get their files back.
Protection against scareware and ransomware would require the common best practices against malware, in particular, users must be cautious and exercise their common sense, and use of legitimate security software is of particular importance. Some best practices for protection against scareware, ransomware, as well as other virus and malicious code attacks are:

- Backup important data frequently and keep the backup data disconnected from the computer
- Refrain from visiting suspicious websites or downloading any files from them
- Do not open any suspicious emails or instant messages, as well as the attachments and hyperlinks inside
- Check and keep your anti-malware program and signatures are up-to-date
- Install the latest patches for software in use
- Disable macros for Microsoft Word, Excel and other office applications by default
- Enable security features of the system and browser

**Virus Hoax**

A virus hoax is a false virus warning, usually in the form of an email message. It suggests the reader to forward the message to others, resulting in a rapidly growing proliferation of emails that may overload systems.

**Mobile Device Virus / Worms**

Like any computing platform, mobile devices are also susceptible to malicious code attacks. Although at present, malicious codes for handheld devices and smart phones are not that common, there is likely to be an increase as the functionality of mobile applications increase and with the wider deployment of these devices.
The open architecture of mobile application development environments, often with extensive software development documentation and tools, also allow attackers to create malicious code for these platforms quite easily.
Malicious code can infect mobile devices in several ways. These include:

- Via email SMS or MMS: a message containing a hyperlink to a malicious code is sent to entice a user to select the link and download the code. Alternatively, the code can be sent in an email as an attached file and infect the device when executed. Similarly, malicious code can also be propagated via MMS messages. SymbOS / Commwarrior.M is a worm that is capable of spreading via MMS messages on Symbian Series 60 devices.
- Via desktop synchronisation: the worm Cxover is one such an example. Cxover is a proof-of-concept worm that can affect both Windows PC and Windows Mobile devices. If it is executed on a Windows Mobile device, it will copy itself to the computer over an ActiveSync connection. If it is executed on a Windows PC, it will search for any handled devices connected over ActiveSync and copy itself to the device.
- Via Bluetooth, Infra-red or Wi-Fi: the first worm capable of spreading via Bluetooth was discovered in June 2004 and was named Cabir. It was a proof-of-concept worm for Symbian OS Series 60 smart phones but it has not been found in the wild since then. The worm required several interactive steps on the part of the recipient in order to execute. An attacker who intentionally sends a malicious program to trick the recipient into accepting it can also exploit the potential weakness of Bluetooth.

**Logic Bombs**

A logic bomb is a program code which is embedded in another program, and can be activated when a certain predefined criteria are met.
For instance, a time bomb will attack a system and erase all data if a licence key or another program code is not found in the system. In some cases, a logic bomb will inform the attacker via the Internet that the bomb is ready to attack the victim.

**Trap Door**

A trap door is a secret entry point into a program that is intentionally included in the program code. While it can facilitate debugging during program development, it may be used for malicious purposes as well.

**Common Obfuscation Techniques**

The following are common obfuscation techniques used by malicious code developers and writers to evade detection and destruction:

- **Binders and Packers**
  Most virus signature files are created based on the checksum value which makes use of the file properties and first few bytes of the malicious code binaries. The binders technique is to bind the virus and malicious code file on to another file, which changes its form. The packers technique is to compress the virus code before it is embedded.

- **Self-Encryption and Self-Decryption**
  Malicious code may encrypt and decrypt itself, even using several layers of encryption and decryption and/or using random keys in encryption and decryption. This makes them harder to examine directly.
- **Polymorphism**
  Malicious code can change its default encryption settings as well as the decryption code during self-encryption. These make it much more difficult to detect.
- **Metamorphism**
  Malicious code change its form by, for instance, rearranging its code fragments or/and by adding useless lines of code into its source, and recompiling itself into a new form.
- **Code conversion to a VB (Visual Basic) script**
  This method converts an executable program (.exe) into a visual basic script (.vbs) file that can be attached to a document, data files or email messages.
- **Stealth**
  The technique is designed to evade anti-virus software detection by hiding the code itself. One example is to monitor system calls to files; the malicious code then modifies the return information to the process call by returning only original information.

## 5. Levels of information Security (Data, Application, Network etc.)

### Level 1

**Public information**

Information that is considered public.

**Examples:**

- Research data that has been de-identified in accordance with applicable rules;
- Published research data; published information about the University;
- Course catalogs;
- Directory information about students who have not requested a FERPA block;
- Faculty and staff directory information.

**Level 2: Information the disclosure of which would not cause material harm, but which the University has chosen to keep confidential.**

**For user**

**No Shared Passwords**

U1: Users' passwords and other access credentials must never be shared.

**Protect Passwords**

U2: All passwords and other access credentials must be protected.

**Different Passwords**

U3: Different passwords must be used for Harvard and non-Harvard accounts.

**Strong Passwords**

U4: Passwords used on all systems for Harvard business should be of sufficient length and complexity to reasonably protect them from being guessed by humans or computers. (Most Harvard systems enforce length and complexity standards.)

**Compromised Passwords**

U5: Passwords must be changed immediately if there is suspicion of compromise.

**Accessing Confidential Information**

U6: Confidential information must only be accessed for authorized purposes.

**Sharing Confidential Information**

U7: Confidential information must only be shared with those authorized to receive it.

**Protecting Devices**

U8: All devices (including desktops, laptops and mobile devices such as smartphones and tablets) storing or processing confidential information must meet Harvard device protection requirements.

**For Devices**

**Configuring User Devices**

D1: All user devices must be configured for secure operation. The device must be configured to limit access to the specific person or persons authorized to use the device.

**Lost Devices**

D2: The information stored on the device must be protected against access if the device is lost or stolen. All mobile devices (laptops, mobile phones, etc.) that may be used to store or access Harvard information, including accessing Harvard email, must be securely configured, including encryption.

**Applying Patches**

D3: Operating system and application patches must be applied promptly.

**Configuring Applications**

D4: Client applications on the device which might be used to access or transfer confidential information must be configured to protect their communications.

**Disposing of Devices**

D5: The information stored on the device must be protected against access when the device is disposed of.

**Reporting Lost Device**

D6: Any actual or suspected loss, theft, or improper use of a device storing confidential information must be reported promptly.

**Device Management Systems**

D7: Anyone deploying or using a device management system other than Blackberry Enterprise Server or Microsoft ActiveSync must contact the University Security Office.

**For Servers**

**Application owner and classification level**

SA1: Server operators must be able to identify a responsible party, known as the business application owner, for each application on the server and the data classification level of the information that the application stores and processes.

**Complex passwords**

SA2: Servers and applications that manage passwords must force the setting of a complex password. This must meet the following requirements where technically feasible (consult the Security office if the following requirements are not technically feasible):... Read moreabout Complex passwords

**Server communication**

SA3: Communications between servers or applications and client machines must be protected.

**Server-application communication**

SA4: Communications between servers or applications must be protected.

**Default passwords and generic accounts**

SA5: Default passwords must be changed and generic accounts must be disabled or removed before the server or application is put into use.

**Appropriate user access**

SA6: Users must only be permitted to access a server or application after their current business need for access has been established.

**Stored passwords**

SA7: Systems that manage user passwords must be designed in such a way that the passwords are not retrievable by administrators.

**Password Management**

SA8: Mechanisms for users to set or change passwords must be secure. Systems that manage passwords must be configured securely. Storage and management of passwords requires L4 security.

**Current patches**

SA9: Operating system and application patches must be current.

**Malware detection**

SA10: Servers must be running applicable malware detection software with up-to-date signature files.

**No shared accounts**

SA11: Server operators must not knowingly permit shared user account credentials.

**Scanning servers**

SA12: All University owned servers must be annually scanned for the presence of High Risk Confidential Information (HRCI).

**Highest classification**

SA13: Servers storing or processing information belonging to more than one classification must meet the requirements associated with the highest classification.

**Server operators**

SA14: People responsible for the operation of servers must have the skills, experience and/or training needed to implement these requirements.

**For Paper/ Physical Records**

**Limiting Access**

P1: Access must be limited to those persons with valid business reasons to access the records.

**Protecting Physical Records**

P2: Records must be locked up when not in active use.

**Transferring Records**

P4: Any physical transfer of records must use means that are appropriately secure and such transfers must be tracked to confirm that they actually reached the intended recipient.

**Destroying Records**

P6: Destruction of records must be accomplished by means that make it impossible to reconstruct the records.

## 6. Application Security Vulnerabilities ( cross-site scripting, buffer overflow etc)

**1. Injection**

Injection flaws, such as SQL injection, LDAP injection, and CRLF injection, occur when an attacker sends untrusted data to an interpreter that is executed as a command without proper authorization.

* **Application security testing** can easily detect injection flaws. Developers should use parameterized queries when coding to prevent injection flaws.

**2. Broken Authentication and Session Management**

Incorrectly configured user and session authentication could allow attackers to compromise passwords, keys, or session tokens, or take control of users' accounts to assume their identities.

* **Multi-factor authentication**, such as FIDO or dedicated apps, reduces the risk of compromised accounts.

**3. Sensitive Data Exposure**

Applications and APIs that don't properly protect sensitive data such as financial data, usernames and passwords, or health information, could enable attackers to access such information to commit fraud or steal identities.

* **Encryption of data at rest and in transit** can help you comply with data protection regulations.

**4. XML External Entity**

Poorly configured XML processors evaluate external entity references within XML documents. Attackers can use external entities for attacks including remote code execution, and to disclose internal files and SMB file shares.

* **Static application security testing (SAST)** can discover this issue by inspecting dependencies and configuration.

**5. Broken Access Control**

Improperly configured or missing restrictions on authenticated users allow them to access unauthorized functionality or data, such as accessing other users' accounts, viewing sensitive documents, and modifying data and access rights.

* **Penetration testing** is essential for detecting non-functional access controls; other testing methods only detect where access controls are missing.

**6. Security Misconfiguration**

This risk refers to improper implementation of controls intended to keep application data safe, such as misconfiguration of security headers, error messages containing sensitive information (information leakage), and not patching or upgrading systems, frameworks, and components.

* **Dynamic application security testing (DAST)** can detect misconfigurations, such as leaky APIs.

**7. Cross-Site Scripting**

Cross-site scripting (XSS) flaws give attackers the capability to inject client-side scripts into the application, for example, to redirect users to malicious websites.

* **Developer training complements security testing** to help programmers prevent cross-site scripting with best coding best practices, such as encoding data and input validation**.**

**8. Insecure deserialization**

Insecure deserialization flaws can enable an attacker to execute code in the application remotely, tamper or delete serialized (written to disk) objects, conduct injection attacks, and elevate privileges.

* **Application security tools can detect deserialization flaws** but penetration testing is frequently needed to validate the problem.

**9. Using Components With Known Vulnerabilities**

Developers frequently don't know which open source and third-party components are in their applications, making it difficult to update components when new vulnerabilities are discovered. Attackers can exploit an insecure component to take over the server or steal sensitive data.

* **Software composition analysis** conducted at the same time as static analysis can identify insecure versions of components.

**10. Insufficient Logging and Monitoring**

The time to detect a breach is frequently measured in weeks or months. Insufficient logging and ineffective integration with security incident response systems allow attackers to pivot to other systems and maintain persistent threats.

*** Think like an attacker** and use pen testing to find out if you have sufficient monitoring; examine your logs after pen testing

## 7. Difference between private and public keys

| Private/Secret key: | Public key: |
|---|---|
| 1. Private key is faster compared to public key<br>2. Private key is symmetrical . Actually there is only one key. the other is a copy of it.<br>3. Private key is truly private .Should be available with only the two communicating parties.<br>4. The two parties must have met before at least once to share the key.<br>5. A secret key that can be used to decrypt messages encrypted with the corresponding public or private key.<br>6. Applies to Asymmetric Encryption & Symmetric Encryption<br>Example: Your private key (Which shouldn't be shared with anyone) is the access to that 'money'<br><br>So If you share you private key. That person can basically help themselves to all the money in that address. | 1. Relatively slow to encrypt/decrypt<br>2. Asymmetrical<br>3. Public key can be made public. Private key is truly secret.<br>4. The two parties need not have met . The two may be strangers, half way around the globe.<br>5. A published key that can be used to send a secure message to a receiver<br>6. Applies to Asymmetric Encryption<br>**Example**: A public key is like an email address. Thats the address you send 'money' to. Just like you would broadcast your email address for someone to contact you. |

## 8. Algorithms: Private ( DES, Triple DES, AES) and public ( RSA)

### RSA

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private key is kept private.

An example of asymmetric cryptography :

1. A client (for example browser) sends its public key to the server and requests for some data.
2. The server encrypts the data using client's public key and sends the encrypted data.
3. Client receives this data and decrypts it.

Since this is asymmetric, nobody else except browser can decrypt the data even if a third party has public key of browser.

A simple, worked example

Alice generates her RSA keys by selecting two primes: p=11 and q=13. The modulus n=p×q=143. The totient of n φ(n)=(p−1)x(q−1)=120. She chooses 7 for her RSA public key eand calculates her RSA private key using the Extended Euclidean Algorithm which gives her 103.

Bob wants to send Alice an encrypted message M so he obtains her RSA public key (n, e) which in this example is (143, 7). His plaintext message is just the number 9 and is encrypted into ciphertext C as follows:

$$Me \bmod n = 97 \bmod 143 = 48 = C$$

When Alice receives Bob's message she decrypts it by using her RSA private key (d, n) as follows:

$$Cd \bmod n = 48103 \bmod 143 = 9 = M$$

To use RSA keys to digitally sign a message, Alice would create a hash or message digest of her message to Bob, encrypt the hash value with her RSA private key and add it to the message. Bob can then verify that the message has been sent by Alice and has not been altered by decrypting the hash value with her public key. If this value matches the hash of the original message, then only Alice could have sent it (authentication and non-repudiation) and the message is exactly as she wrote it (integrity). Alice could, of course, encrypt her message with Bob's RSA public key (confidentiality) before sending it to Bob. A digital certificate contains information that identifies the certificate's owner and also contains the owner's public key. Certificates are signed by the certificate authority that issues them, and can simplify the process of obtaining public keys and verifying the owner.

### AES

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows −

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

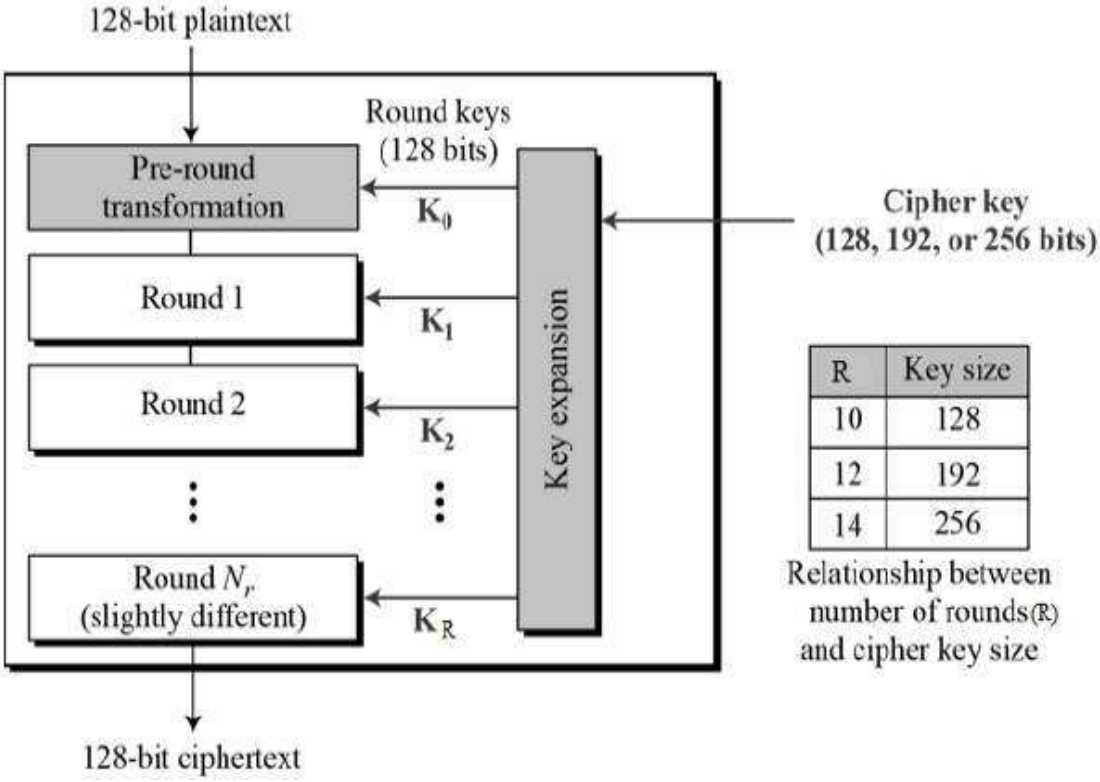
**Operation of AES**

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The schematic of AES structure is given in the following illustration −

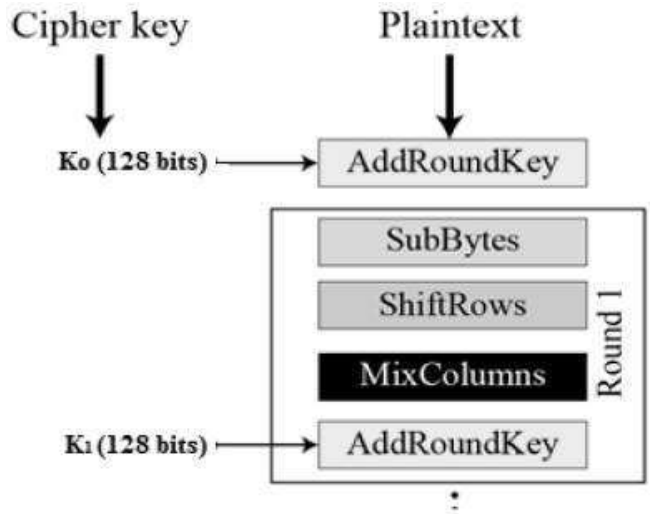



| R | Key size |
|---|---|
| 10 | 128 |
| 12 | 192 |
| 14 | 256 |

Relationship between number of rounds (R) and cipher key size

**Encryption Process**

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below −




**Byte Substitution (SubBytes)**

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

**Shiftrows**

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows −

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

**MixColumns**

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

**Addroundkey**

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

**Decryption Process**

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order −

- Add round key
- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related.

**AES Analysis**

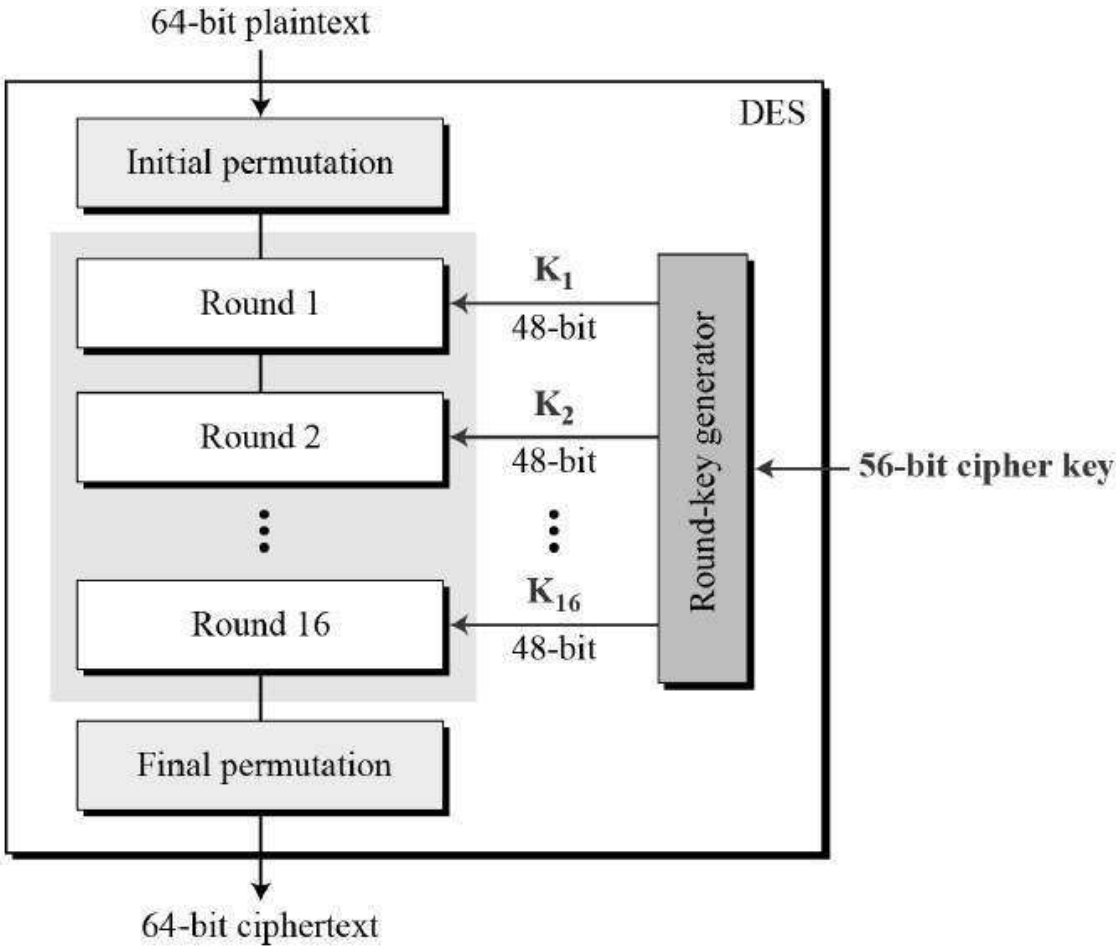
In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of 'future-proofing' against progress in the ability to perform exhaustive key searches.

However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.

## DES

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

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). General Structure of DES is depicted in the following illustration −

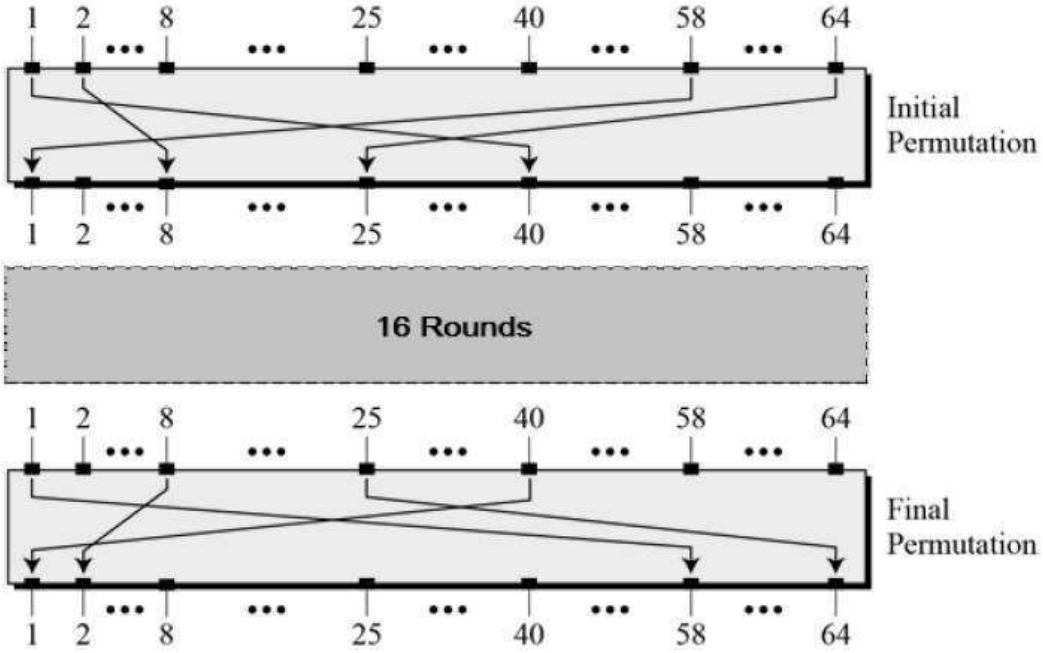



Since DES is based on the Feistel Cipher, all that is required to specify DES is −

- Round function
- Key schedule
- Any additional processing − Initial and final permutation

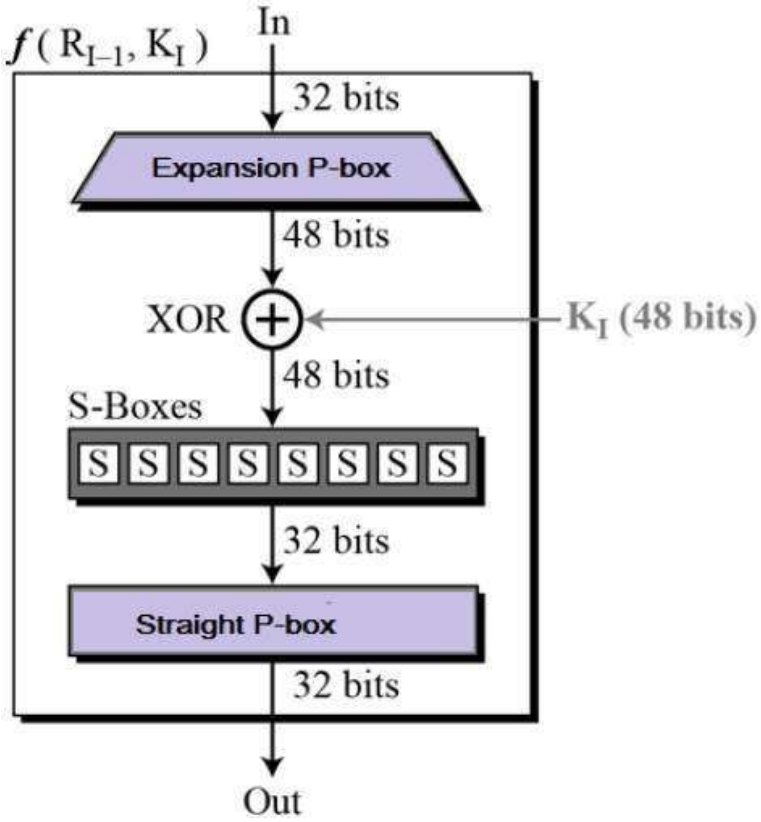
**Initial and Final Permutation**

The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES. The initial and final permutations are shown as follows −

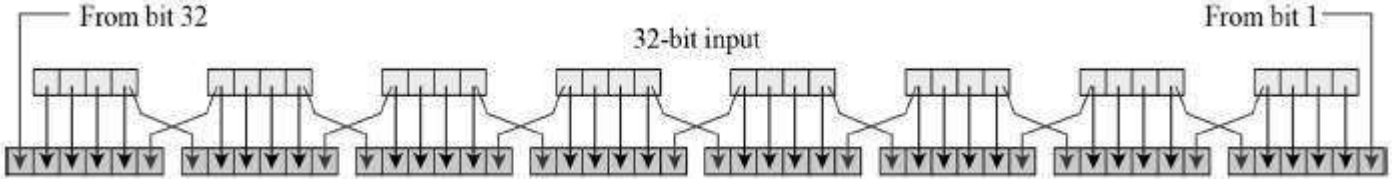


**Round Function**

The heart of this cipher is the DES function, *f*. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.



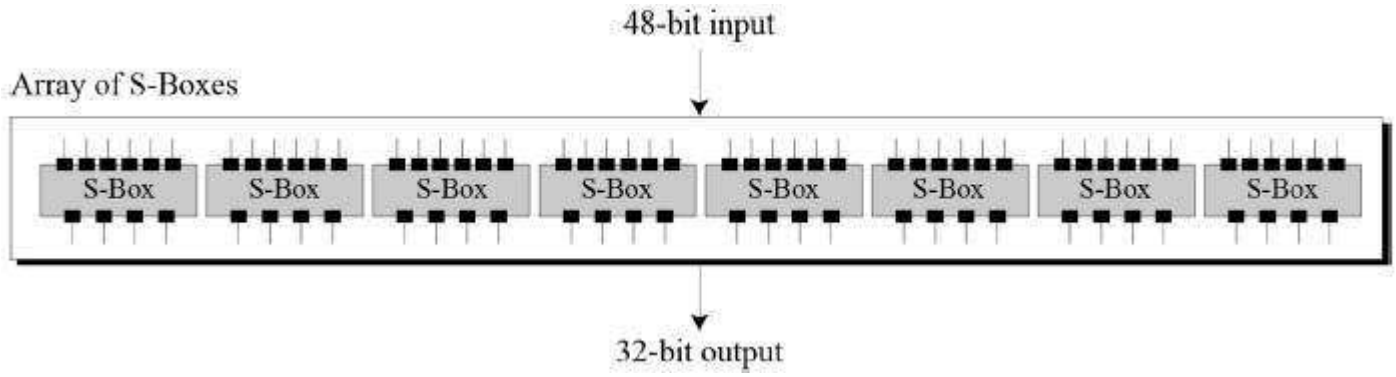

- **Expansion Permutation Box** – Since right input is 32-bit and round key is a 48-bit, we first need to expand right input to 48 bits. Permutation logic is graphically depicted in the following illustration –



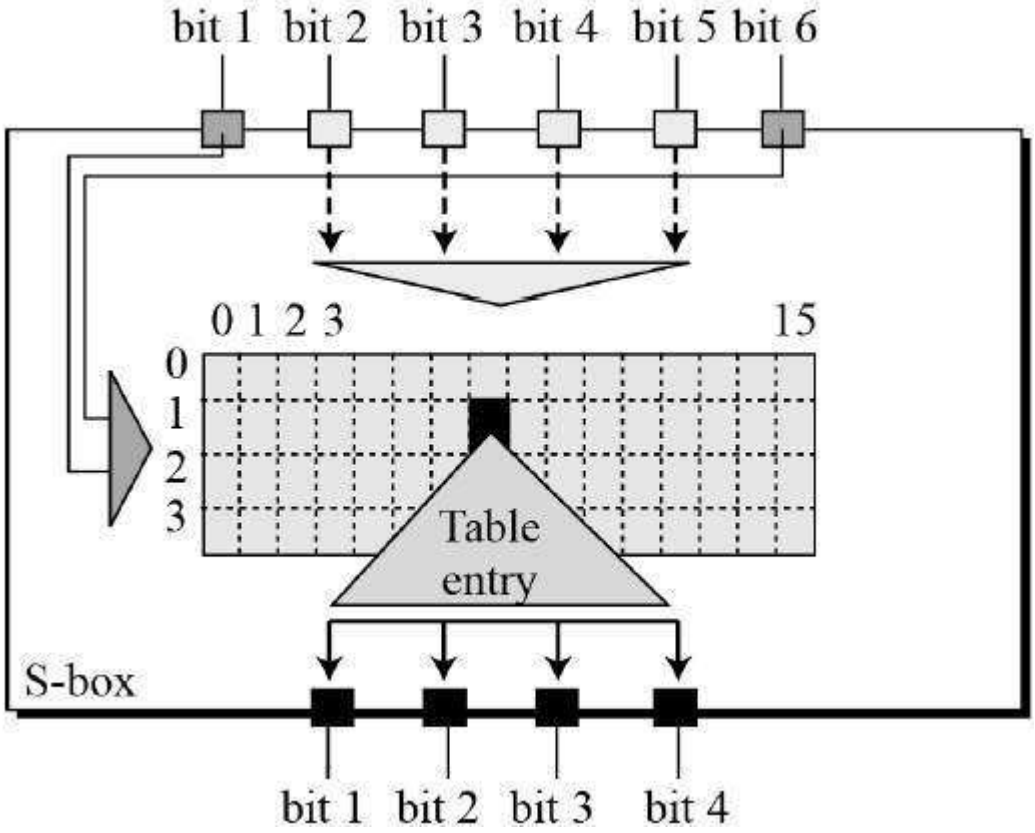

- The graphically depicted permutation logic is generally described as table in DES specification illustrated as shown –

| | | | | | |
|---|---|---|---|---|---|
| 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 |

- **XOR (Whitener).** – After the expansion permutation, DES does XOR operation on the expanded right section and the round key. The round key is used only in this operation.
- **Substitution Boxes.** – The S-boxes carry out the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output. Refer the following illustration –




- The S-box rule is illustrated below −

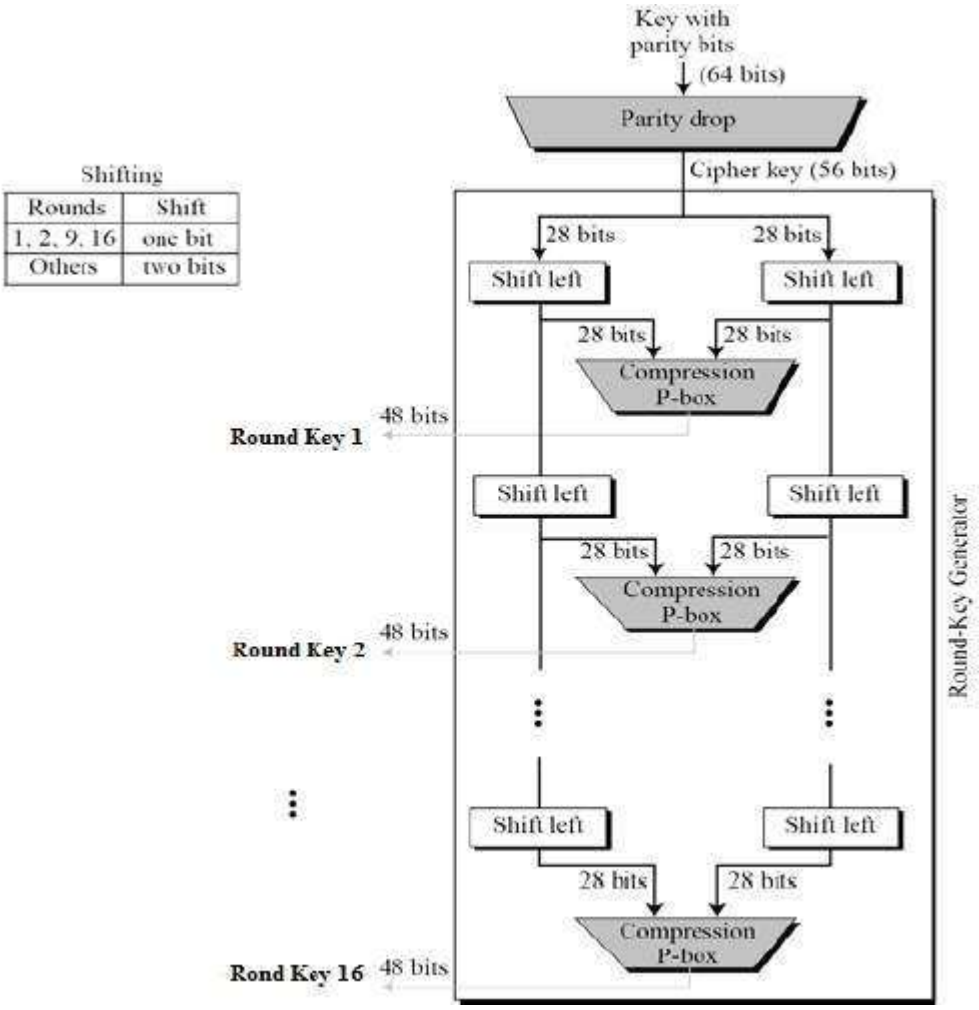



- There are a total of eight S-box tables. The output of all eight s-boxes is then combined in to 32 bit section.
- **Straight Permutation** − The 32 bit output of S-boxes is then subjected to the straight permutation with rule shown in the following illustration:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 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 |

**Key Generation**

The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key. The process of key generation is depicted in the following illustration −




The logic for Parity drop, shifting, and Compression P-box is given in the DES description.

**DES Analysis**

The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong.

- **Avalanche effect** − A small change in plaintext results in the very great change in the ciphertext.
- **Completeness** − Each bit of ciphertext depends on many bits of plaintext.

During the last few years, cryptanalysis have found some weaknesses in DES when key selected are weak keys. These keys shall be avoided.

DES has proved to be a very well designed block cipher. There have been no significant cryptanalytic attacks on DES other than exhaustive key search.

**3DES**

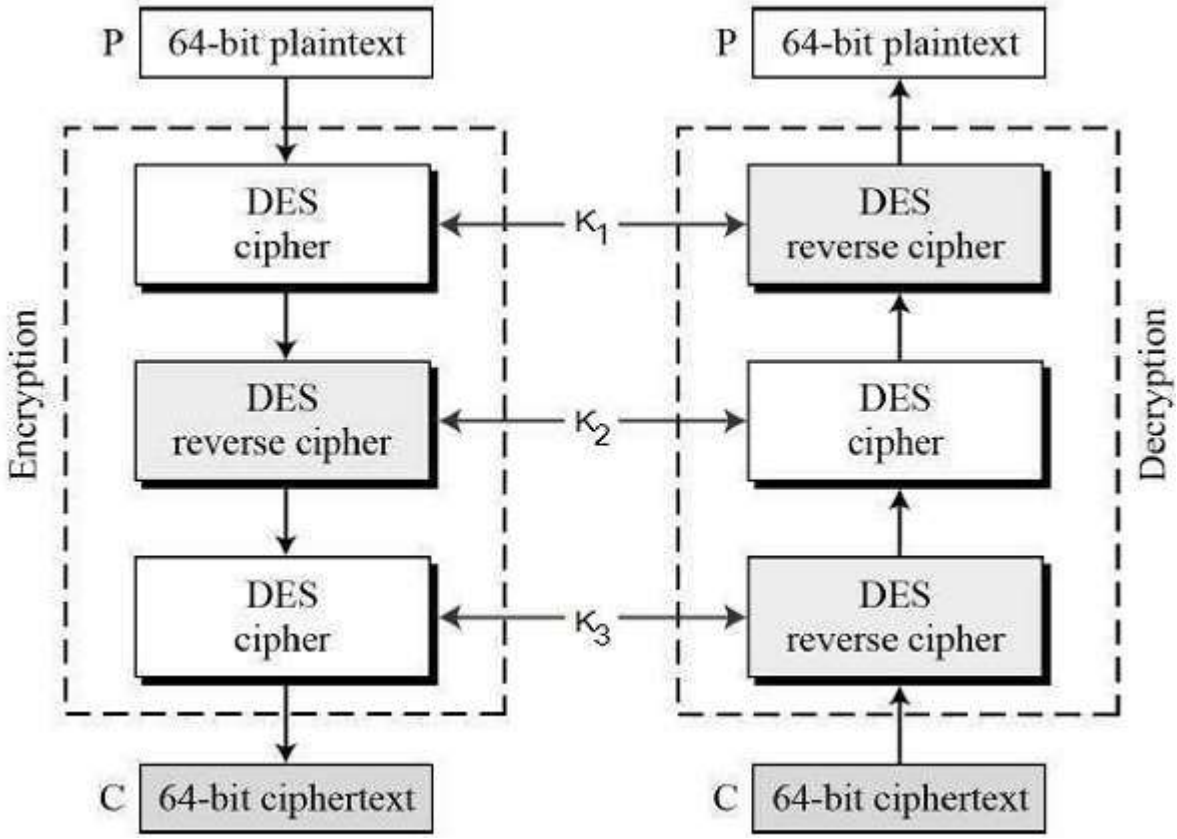
The speed of exhaustive key searches against DES after 1990 began to cause discomfort amongst users of DES. However, users did not want to replace DES as it takes an enormous amount of time and money to change encryption algorithms that are widely adopted and embedded in large security architectures.

The pragmatic approach was not to abandon the DES completely, but to change the manner in which DES is used. This led to the modified schemes of Triple DES (sometimes known as 3DES).

Incidentally, there are two variants of Triple DES known as 3-key Triple DES (3TDES) and 2-key Triple DES (2TDES).

**3-KEY Triple DES**

Before using 3TDES, user first generate and distribute a 3TDES key K, which consists of three different DES keys $K_1$, $K_2$ and $K_3$. This means that the actual 3TDES key has length 3×56 = 168 bits. The encryption scheme is illustrated as follows −




The encryption-decryption process is as follows −

- Encrypt the plaintext blocks using single DES with key $K_1$.
- Now decrypt the output of step 1 using single DES with key $K_2$.
- Finally, encrypt the output of step 2 using single DES with key $K_3$.
- The output of step 3 is the ciphertext.
- Decryption of a ciphertext is a reverse process. User first decrypt using $K_3$, then encrypt with $K_2$, and finally decrypt with $K_1$.

Due to this design of Triple DES as an encrypt–decrypt–encrypt process, it is possible to use a 3TDES (hardware) implementation for single DES by setting $K_1$, $K_2$, and $K_3$ to be the same value. This provides backwards compatibility with DES.

Second variant of Triple DES (2TDES) is identical to 3TDES except that $K_3$is replaced by $K_1$. In other words, user encrypt plaintext blocks with key $K_1$, then decrypt with key $K_2$, and finally encrypt with $K_1$ again. Therefore, 2TDES has a key length of 112 bits.

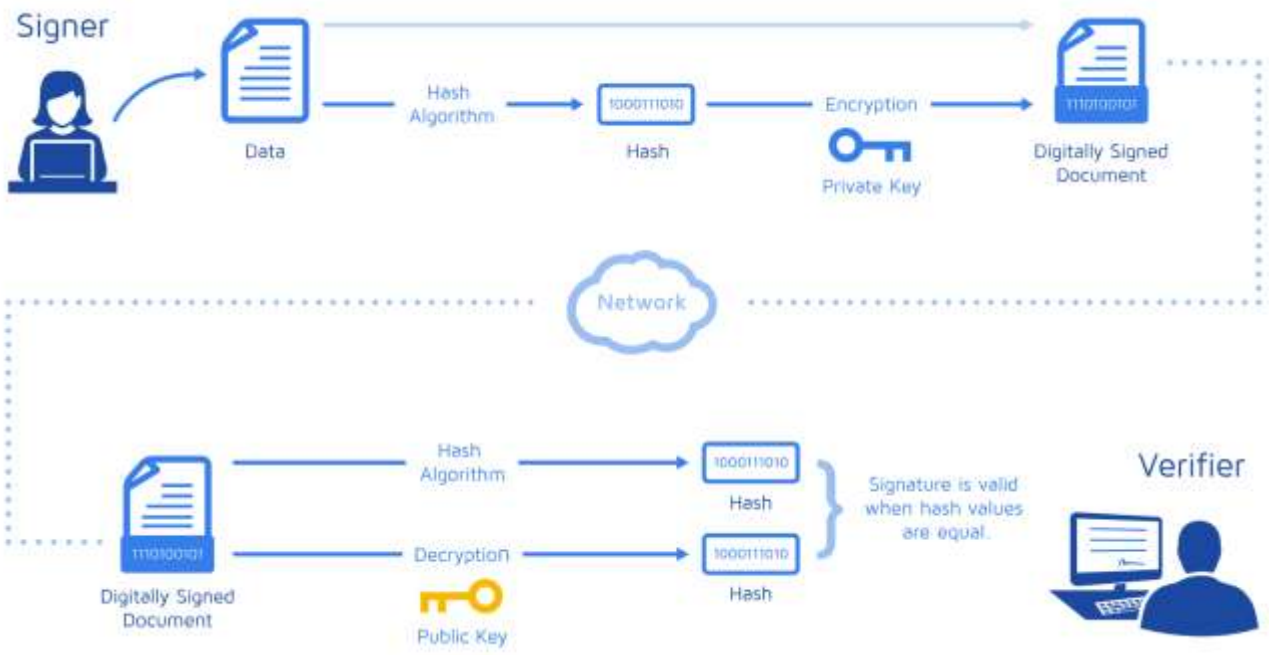
Triple DES systems are significantly more secure than single DES, but these are clearly a much slower process than encryption using single DES.

## 9. Hash Function and message digest

**The basic difference between a hash function and digest is that digest is the value obtained from a hash function.**

- A hash function is any function that can be used to map data of arbitrary size to data of fixed size. **The values returned by a hash function are called hash values, hash codes, digests, or** simply **hashes**.
- One use is a data structure called a hash function, widely used in computer software for rapid data lookup. For example, suppose that you want to count the number of occurrences of the alphabets in a string.
- Always remember that the hash digest returns an alphanumeric message which is the digest. Also,the hash function tries to map large data of variable length to a fixed length data.

## 10. Digital Signature and PKI




**How do I create a digital signature?**

eSignature providers, such as DocuSign, that offer solutions based on digital signature technology, make it easy to digitally sign documents. They provide an interface for sending and signing documents online and work with the appropriate Certificate Authorities to provide trusted digital certificates.

Depending upon the Certificate Authority you are using, you may be required to supply specific information. There also may be restrictions and limitations on whom you send documents to for signing and the order in which you send them. DocuSign's interface walks you through the process and ensures that you meet all of these requirements. When you receive a document for signing via email, you must authenticate as per the Certificate Authority's requirements and then "sign" the document by filling out a form online.

**What is Public Key Infrastructure (PKI)?**

Public Key Infrastructure (PKI) is a set of requirements that allow (among other things) the creation of digital signatures. Through PKI, each digital signature transaction includes a pair of keys: a private key and a public key. The private key, as the name implies, is not shared and is used only by the signer to electronically sign documents. The public key is openly available and used by those who need to validate the signer's electronic signature. PKI enforces additional requirements, such as the Certificate Authority (CA), a digital certificate, end-user enrollment software, and tools for managing, renewing, and revoking keys and certificates.

**What is a Certificate Authority (CA)?**

Digital signatures rely on public and private keys. Those keys have to be protected in order to ensure safety and to avoid forgery or malicious use. When you send or sign a document, you need assurance that the documents and the keys are created securely and that they are using valid keys. CAs, a type of Trust Service Provider, are third-party organizations that have been widely accepted as reliable for ensuring key security and that can provide the necessary digital certificates. Both the entity sending the document and the recipient signing it must agree to use a given CA.

DocuSign is also a CA when signers sign using the DocuSign Express Digital Signature. That means you can always send a document with a digital signature by using DocuSign as the Certificate Authority. Alternatively, you can securely establish your own CA using the DocuSign Signature Appliance and still access the rich features of DocuSign cloud services for transaction management. Some organizations or regions rely on other prominent CAs, and the DocuSign platform supports them, as well. These include OpenTrust, which is widely used in European Union countries, and SAFE-BioPharma, which is an identity credential that life science organizations may elect to use.

**Why would I use a digital signature?**

Many industries and geographical regions have established eSignature standards that are based on digital signature technology, as well as specific certified CAs, for business documents. Following these local standards based on PKI technology and working with a trusted certificate authority can ensure the enforceability and acceptance of an e-signature solution in each local market. By using the PKI methodology, digital signatures utilize an international, well-understood, standards-based technology that also helps to prevent forgery or changes to the document after signing.

**What digital signature solutions does DocuSign offer?**

DocuSign Standards-Based Signatures enable you to automate and manage entire digital workflows using DocuSign's powerful business capabilities while staying compliant with local and industry eSignature standards, including CFR Part 11 and the EU eIDAS regulation. In the EU, DocuSign delivers all of the signature types defined under eIDAS, including EU Advanced Electronic Signatures (AdES) and EU Qualified Electronic Signatures (QES).

**Are eSignatures, based on digital signature technology, legally enforceable?**

Yes. The EU passed the EU Directive for Electronic Signatures in 1999, and the United States passed the Electronic Signatures in Global and National Commerce Act (ESIGN) in 2000. Both acts made electronically signed contracts and documents legally binding, like paper-based contracts. Since then, the legality of electronic signatures has been upheld many times.

By now, most countries have adopted legislation and regulations modeled after the United States or the European Union, with a preference in many regions for the E.U. model of locally managed, digital signature technology-based eSignatures. In addition, many companies have improved compliance with the regulations established by their industries (e.g., FDA 21 CFR Part 11 in the Life Sciences industry), which has been achieved by using digital signature technology. These country- and industry-specific regulations are continuously evolving, a key example being the Electronic identification and trust services (eIDAS) regulation that was recently adopted in the European Union.

**What is a digital certificate?**

A digital certificate is an electronic document issued by a Certificate Authority (CA). It contains the public key for a digital signature and specifies the identity associated with the key, such as the name of an organization. The certificate is used to confirm that the public key belongs to the specific organization. The CA acts as the guarantor. Digital certificates must be issued by a trusted authority and are only valid for a specified time. They are required in order to create a digital signature.

## 11. Comparison between symmetric and asymmetric cryptosystem

- Symmetric encryption uses a single key that needs to be shared among the people who need to receive the message while asymmetrical encryption uses a pair of public key and a private key to encrypt and decrypt messages when communicating.
- Symmetric encryption is an old technique while asymmetric encryption is relatively new.
- Asymmetric encryption was introduced to complement the inherent problem of the need to share the key in symmetrical encryption model, eliminating the need to share the key by using a pair of public-private keys.
- Asymmetric encryption takes relatively more time than the symmetric encryption.

## 12. Concept of Identification, Authentication and Authorization

**Identification**

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

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

**Authentication**

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

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

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

**Authorization**

Authorization is what takes place after a person has been both identified and authenticated; it's the step determines what a person can then do on the system.

An example in people terms would be someone knocking on your door at night. You say, "Who is it?", and wait for a response. They say, "It's John." in order to identify themselves. You ask them to back up into the light so you can see them through the peephole. They do so, and you authenticate them based on what they look like (biometric). At that point you decide they can come inside the house.

If they had said they were someone you didn't want in your house (identification), and you then verified that it was that person (authentication), the authorization phase would not include access to the inside of the house.

## 13. Authentication methods (2 factor, 3-factor etc.)

- **One-factor authentication** – this is "something a user knows." The most recognized type of one-factor authentication method is the password.
- **Two-factor authentication** – in addition to the first factor, the second factor is "something a user has." Examples of something a user has are a fob that generates a pre-determined code, a signed digital certificate or even a biometric such as a fingerprint. The most recognized form of two-factor authentication is the ubiquitous RSA SecurID fob.
- **Three-factor authentication** – in addition to the previous two factors, the third factor is "something a user is." Examples of a third factor are all biometric such as the user's voice, hand configuration, a fingerprint, a retina scan or similar. The most recognized form of three-factor authentication is usually the retina scan.

## 14. Authorization techniques

**Authorization**

- Determines that the proven identity has some set of characteristics associated with it that gives it the right to access the requested resources.
- Granting access rights to subjects should be based on the level of trust a company has in a subject and the subject's need to know.
- Is a core component of every operating system and established whether a user is authorized to access a particular resource and what actions he is permitted to perform on the resource

**Access Criteria can be thought of as:**

- **Roles**: Is an efficient way to assign rights to a type of user who performs a certain task. ( job assignment or function).
- **Groups**: When several users require same type of access to information and resources
- **Location**: To restrict unauthorized individuals from being able to get in and reconfigure the server remotely.
- **Time**: Restrict the times that certain actions or services can be accessed.
- **Transaction Types:** Can be used to control what data is accessed during certain types of functions and what commands can be carried out on the data.

**Authorization concepts to keep in mind:**

- **Authorization Creep:** When new access rights and permissions assigned to employee without the old permissions being reviewed and removed.
- **Default to Zero:** All access controls should be based on the concept of starting with zero access and then building on top of that.
- **Need to Know Principle:** individuals should be given access only to the information that they absolutely require in order to complete their job duties.
- **Access Control Lists:** A list of subjects that are authorized to access a particular object.

**Solutions that enterprise wide and single sign on solutions supply:**

- User provisioning
- Password synchronization and reset
- Self service
- Centralized auditing and reporting
- Integrated workflow (increase in productivity)
- Regulatory compliance

**Single Sign On Capabilities:** Allow user credentials to be entered one time and the user is then able to access all resources in primary and secondary network domains. SSO technologies include:

- **Kerberos**
  - An SSO open-standards protocol for authentication in a single security domain.
  - Kerberos is an authentication protocol that uses symmetric key encryption in three key pairs: two authentication pairs are shared by the authenticator and a single principal and one session pair is shared between principals.
  - The session-key pair is distributed in such a way that principals are required to trust the authenticator rather than each other.
- **Sesame:** The Secure European System for Applications in a Multi-Vendor Environment (SESAME) is a protocol developed by the European Union that addresses multiple or disparate security domains.
- Security Domains

- Directory Services
- Dumb Terminals

➢ **SISO Pros :**

- Efficient log-on process -The user logs on only once to access all authorized systems.
- Encourages users to create stronger passwords -With only one password to remember and control, users may be inclined to use passwords that are harder and more difficult to crack. Fewer passwords to manage should also result in fewer being written down in unsafe locations.
- Centralized administration -Ensures consistent application of policy and procedures.

➢ **SISO Cons :**

- Single point of compromise -A single compromised sign-in allows the intruder into all of the account owner‟s authorized resources.
- Legacy Interoperability-It may be difficult to include unique computers or legacy systems in the single sign on network.
- Implementation difficulties-Unusual types of systems may not interface well with SSO software.

## 15. Access control models ( Discretionary, mandatory and Role Based)

### a. Discretionary

Discretionary access control (DAC) is a type of security access control that grants or restricts object access via an access policy determined by an object's owner group and/or subjects. DAC mechanism controls are defined by user identification with supplied credentials during authentication, such as username and password. DACs are discretionary because the subject (owner) can transfer authenticated objects or information access to other users. In other words, the owner determines object access privileges.

In DAC, each system object (file or data object) has an owner, and each initial object owner is the subject that causes its creation. Thus, an object's access policy is determined by its owner.

A typical example of DAC is Unix file mode, which defines the read, write and execute permissions in each of the three bits for each user, group and others.

DAC attributes include:

- User may transfer object ownership to another user(s).
- User may determine the access type of other users.
- After several attempts, authorization failures restrict user access.
- Unauthorized users are blind to object characteristics, such as file size, file name and directory path.
- Object access is determined during access control list (ACL) authorization and based on user identification and/or group membership.

DAC is easy to implement and intuitive but has certain disadvantages, including:

- Inherent vulnerabilities (Trojan horse)
- ACL maintenance or capability
- Grant and revoke permissions maintenance
- Limited negative authorization power

### b. Mandatory

- Mandatory access control (MAC) is a security strategy that restricts the ability individual resource owners have to grant or deny access to resource objects in a file system. MAC criteria are defined by the system administrator, strictly enforced by the operating system (OS) or security kernel, and are unable to be altered by end users.
- Often employed in government and military facilities, mandatory access control works by assigning a classification label to each file system object. Classifications include confidential, secret and top secret. Each user and device on the system is assigned a similar classification and clearance level. When a person or device tries to access a specific resource, the OS or security kernel will check the entity's credentials to determine whether access will be granted. While it is the most secure access control setting available, MAC requires careful planning and continuous monitoring to keep all resource objects' and users' classifications up to date.
- As the highest level of access control, MAC can be contrasted with lower-level discretionary access control (DAC), which allows individual resource owners to make their own policies and assign security controls.

### c. Non-Discretionary (Role Based)

A "non-discretionary access control" system is means of access control where the owner of the securable does not explicitly define the individuals that can access it. Rather, it will rely on a set of rules, privileges, or roles to provide access.
Some real life scenarios would be:

1. A gate that unlocks between 8am-8pm daily (Rule-Based Access)
2. A user with an administrator role that can access the settings of an application (Role-Based Access)
3. A person with a specific security-clearance level, accessing a document that is classified to a specific level (Rule+Role)

**Discretionary Access Control vs Mandatory Access Control**

**Discretionary Access Control**

- In discretionary access control (DAC), the owner of the object specifies which subjects can access the object. This model is called discretionary because the control of access is based on the discretion of the own
- Most operating systems such as all Windows, Linux, and Macintosh and most flavors of Unix are based on DAC models.
- In these operating systems, when you create a file, you decide what access privileges you want to give to other users; when they access your file, the operating system will make the access control decision based on the access privileges you created.

**Mandatory Access Control**

- In mandatory access control (MAC), the system (and not the users) specifies which subjects can access specific data objects.
- The MAC model is based on security labels. Subjects are given a security clearance (secret, top secret, confidential, etc.), and data objects are given a security classification (secret, top secret, confidential, etc.). The clearance and classification data are stored in the security labels, which are bound to the specific subjects and objects.
- When the system is making an access control decision, it tries to match the clearance of the subject with the classification of the object. For example, if a user has a security clearance of secret, and he requests a data object with a security classification of top secret, then the user will be denied access because his clearance is lower than the classification of the object.
- The MAC model is usually used in environments where confidentiality is of utmost importance, such as a military institution.
- Examples of the MAC-based commercial systems are SE Linux and Trusted Solaris.

## 16. Centralized access control ( RADIUS, TACAS and Diameter)

**RADIUS (Remote Authentication Dial-In User Service)**

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics. Created by Livingston (now owned by Lucent), RADIUS is a de facto industry standard used by a number of network product companies and is a proposed IETF standard.

**Terminal access controller access control system (TACACS)**

- It is an authentication protocol used for remote communication with any server housed in a UNIX network. TACACS provides an easy method of determining user network access via remote authentication server communication. The TACACS protocol uses port 49 by default.
- TACACS uses allow/deny mechanisms with authentication keys that correspond with usernames and passwords. Cisco, which designed and launched the TACACS protocol, is also its owner.
- The TACACS protocol, which has a very simple working mechanism, accepts a user query from a remote server and forwards this query for necessary action to the authentication server. The authentication server may allow or deny a user query on the host's behalf. The host is a system or platform that runs on the server. The query result is sent to the query initiator as a feedback response.
- The routing node used in dialup connections during the user login process allows or denies user access based on the query's response.

**Diameter**

Diameter is a next-generation industry-standard protocol used to exchange authentication, authorization and accounting (AAA) information in Long-Term Evolution (LTE) and IP Multimedia Systems (IMS) networks. It was derived from and improves upon the widely deployed RADIUS (Remote Authentication Dial-In User Service) and LDAP (Lightweight Directory Access Protocol) AAA protocols, providing more reliable, secure and flexible transport mechanisms for mobile data networks. A variety of LTE and IMS network functions make use of Diameter, including the Policy and Charging Rules Function (PCRF), Home Subscriber Server (HSS) and Online Charging System (OCS) elements. The protocol provides a general framework for exchanging AAA messages, and specifies a standard set of AAA request and response commands and attributes.

**Diameter Protocol Advantages:**

- A peer-to-peer architecture for greater flexibility
- Reliable transmission of AAA messages over TCP or SCTP

- Built-in failover mechanisms to guarantee message delivery
- Secure transmission of AAA messages using TLS or IPSec

## 17. Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)

**IDS**

An intrusion detection system (IDS) is a type of security software designed to automatically alert administrators when someone or something is trying to compromise information system through malicious activities or through security policy violations. An IDS works by monitoring system activity through examining vulnerabilities in the system, the integrity of files and conducting an analysis of patterns based on already known attacks. It also automatically monitors the Internet to search for any of the latest threats which could result in a future attack.

There are a multiple ways detection is performed by an IDS. In signature-based detection, a pattern or signature is compared to previous events to discover current threats. This is useful for finding already known threats, but does not help in finding unknown threats, variants of threats or hidden threats.

Another type of detection is anomaly-based detection, which compares the definition or traits of a normal action against characteristics marking the event as abnormal.

**Types of an IDS:**

- **Network Intrusion Detection System (NIDS):** This does analysis for traffic on a whole subnet and will make a match to the traffic passing by to the attacks already known in a library of known attacks.
- **Network Node Intrusion Detection System (NNIDS):** This is similar to NIDS, but the traffic is only monitored on a single host, not a whole subnet.
- **Host Intrusion Detection System (HIDS):** This takes a "picture" of an entire system's file set and compares it to a previous picture. If there are significant differences, such as missing files, it alerts the administrator.
- **Signature-based intrusion detection systems** monitor all the packets traversing the network and compares them against a database of signatures or attributes of known malicious threats, much like antivirus software.
- **Anomaly-based intrusion detection systems** monitor network traffic and compare it against an established baseline, to determine what is considered normal for the network with respect to bandwidth, protocols, ports and other devices. This type of IDS alerts administrators to potentially malicious activity.

**IPS**

- An intrusion prevention system (IPS) is a system that monitors a network for malicious activities such as security threats or policy violations. The main function of an IPS is to identify suspicious activity, and then log information, attempt to block the activity, and then finally to report it.
- Intrusion prevention systems are also known as intrusion detection prevention systems (IDPS).
- An IPS can be either implemented as a hardware device or software. Ideally (or theoretically) and IPS is based on a simple principle that dirty traffic goes in and clean traffic comes out.
- Intrusion prevention systems are basically extensions of intrusion detection systems. The major difference lies in the fact that, unlike intrusion detection systems, intrusion prevention systems are installed are able to actively block or prevent intrusions that are detected. For example, an IPS can drop malicious packets, blocking the traffic an offending IP address, etc.

## 18. Concept of Firewall, firewall types

- A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
- Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.
- A firewall can be hardware, software, or both.

**Types**

- **Packet filter firewall:**

The Packet Filtering Firewall is one of the most basic firewalls. The first step in protecting internal users from the external network threats is to implement this type of security. The first ever firewalls used were of packet filtering type only. As the trends of network threats started changing, so did the firewall building strategies. Most of the routers have packet filtering built-in, but the problem with the routers is that, they are difficult to configure and don't provide extensive logs of the incidents. In my previous firewall tutorials I talked about firewall policies and few other things. That information is also used while designing such firewalls.

To start with the network security, the packet filtering firewalls are the way to go. This functinality is still the main aim of most of the commercial and non-commercial firewalls. As you know by the definition and the purpose of the firewall, the firewall is the first destination for the traffic coming to your internal network. So, anything which comes to your internal network, passes through the

firewall. Of course, reverse is also true. Any outgoing traffic will also pass through the firewall before leaving your network completely. This is the reason that sometimes this type of firewall filter is also called **screening routers**.

**Types of Packet Filtering**

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

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

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

**Stateless Packet Filtering**

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

**Stateful Packet Filtering**

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

**What Should Be Inspected In A Packet Header**

In a packet header few of the possible things which should be checked are:

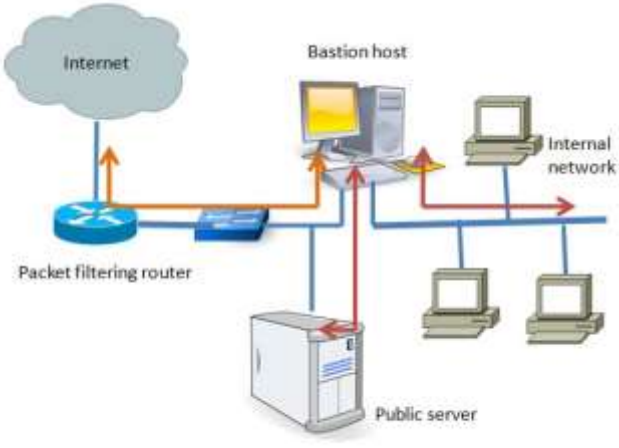
- Source IP address of the packet. This is necessary because IP spoofers might have changed the source IP address to reflect the origin of packet from somewhere else, rather than reflecing the original source.
- Destination IP Address. The firewall rules should check for IP address rather than DNS names. This prevents abuse of DNS servers.
- IP Protocol ID.
- TCP/UDP port number.
- ICMP message type.
- Fragmentation flags.
- IP Options settings.

**Important Features of Packet Filters**

The great firewalls normally follow few specific rules upon which features are incorporated during firewall designing. Few are listed below:

- The firewall should provide good deal of logs. The more detailed are the logs, the better the protection.
- The command line syntax or GUI of firewall should be easy to create new rules and of course firewall exceptions.
- The packet filter orders should be evaluated carefully in order to make the filtering fruiteful.

- **Proxy servers firewall:** An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network. However, this also may impact throughput capabilities and the applications they can support.
- **Screening routers:** A screening router is the basic component of most firewalls. A screening router can be a commercial router or a host-based router with some kind of packet-filtering capability. Typical screeing routers have the ability to block traffic between networks or specific hosts, on an IP port level. Some firewalls consist of nothing more than a screening router.
  The packet-filtering can be done on IP and/or TCP/UDP level. For filtrerig, the router looks at the ip-number, port-number and protocol for each packet it recives. Based on a given set of rules the router decides if it should block, allow or if it needs more rules to decide what to do with a packet. It is usually not easy to set up an consistent list of rules, and the rules mostly get rather complex.
- **Secure bastion hosts**




Screened host firewall ( Dual-homed bastion host)

- A bastion host is a specialized computer that is deliberately exposed on a public network. From a secured network perspective, it is the only node exposed to the outside world and is therefore very prone to attack. It is placed outside the firewall in single firewall systems or, if a system has two firewalls, it is often placed between the two firewalls or on the public side of a demilitarized zone (DMZ).
- The bastion host processes and filters all incoming traffic and prevents malicious traffic from entering the network, acting much like a gateway. The most common examples of b astion hosts are mail, domain name system, Web and File Transfer Protocol (FTP) servers. Firewalls and routers can also become bastion hosts.
- The bastion host node is usually a very powerful server with improved security measures and custom software. It often hosts only a single application because it needs to be very good at what it does. The software is usually customized, proprietary and not available to the public. This host is designed to be the strong point in the network to protect the system behind it. Therefore, it often undergoes regular maintenance and audit. Sometimes bastion hosts are used to draw attacks so that the source of the attacks may be traced.
- To maintain the security of bastion hosts, all unnecessary software, daemons and users are removed. The operating system is continually updated with the latest security updates and an intrusion detection system is installed.

- **Authentication server**

An authentication server is an application that facilitates authentication of an entity that attempts to access a network. Such an entity may be a human user or another server. An authentication server can reside in a dedicated computer, an Ethernet switch, an access point or a network access server.

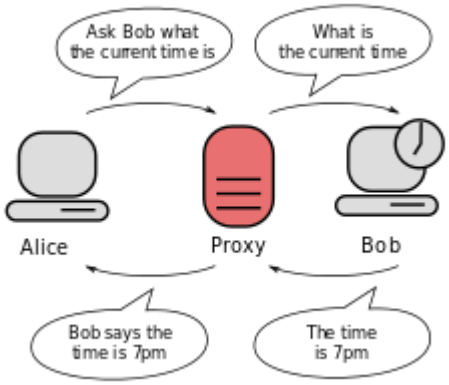
Authentication is the process of determining whether someone or something is actually who or what it declares itself to be. When a potential subscriber accesses an authentication server, a username and password may be the only identifying data required. In a more sophisticated system called Kerberos, the subscriber must request and receive an encrypted security token that can be used to access a particular service. RADIUS (Remote Authentication Dial-In User Service) is a commonly used authentication method. TACACS+ (Terminal Access Controller Access Control System Plus) is similar to RADIUS but is used with Unix networks. RADIUS employs UDP (User Datagram Protocol) and TACACS+ employs TCP (Transmission Control Protocol.

## 19. Proxy server

A proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity. Proxies were invented to add structure and encapsulation to distributed systems. Today, most proxies are web proxies, facilitating access to content on the World Wide Web, providing anonymity and may be used to bypass IP address blocking.

**Uses**

- Monitoring and filtering
  - Content-control software
  - Filtering of encrypted data
  - Bypassing filters and censorship
  - Logging and eavesdropping
- Improving performance
- Translation
- Accessing services anonymously
  - QA geotargeted advertising
- Security
  - Cross-domain resources
- Secondary market brokers




## 20. Network Infrastructure Security

Network infrastructure can be a good investment if you know how to take care of it. Keeping it secure may not be an easy task, but its' well worth it in the end. Outlined below are nine important ways you can make sure that your network remains an asset rather than a liability.

- **Understand your network design:** Unless you know how the infrastructure works, you're in a dead zone. Knowing how data flows from system to system and how devices receive and transmit signals are key points to protecting your network. If you don't have a good grasp of these concepts, you can't successfully secure your network just yet. This is the first crucial step in the process.

- **Review your applications.:** Your network can be infected through the different applications that run in your system. That is why it is important to review your digital applications and monitor them constantly to guarantee that they are safe and secure. Scan your devices for viruses and malware so as not to make your entire infrastructure vulnerable to malicious attacks. Implement a virus protection that prevents worms, viruses, and trojans from entering your system via the web.
- **Find holes in your network:** Every network has at least one weak link, and your job is to find yours early to prevent critical data from leaking. You don't want your company's intellectual properties to be accessed by people who are not supposed to get a hold of them. It's wise to document all your network connections and make sure that things are where they're supposed to be. Review your security policies and protect every device.
- **Build a firewall:** Raising a firewall is possibly the most important measure you should take when securing your network. A firewall serves as a border control that defines your perimeter. It prevents the unauthorized access to your private network, even if the access attempt comes from the inside. Learn how a firewall works and understand the extent of its coverage. Although a firewall can't protect your network 100%, it can surely reduce the risk of security breach in your system.

*As much as possible, keep your network infrastructure simple.Unless a service or device is a staple in your business, it's probably just making your network infrastructure weaker.*

- **Control circumventors:** No security policy is perfect. Even firewalls can be thwarted by what is known as circumventors. These circumventors may come in different forms. They go around security policies and give unauthorized users access to networks that they're not supposed to rack up. Even when there are filters in the networks security control, circumventors can still allow unwanted traffic to visit a certain site. You can't really stop these sophisticated entities, but you can control how they impact your network. Constantly monitor and track your traffic so you can intercept when a circumventor is meddling in your system. You may not be able to prevent the attack, but you may do something about its aftermath.
- **Use Secure Socket Layer:** An SSL or Secure Socket Layer is a protocol that establishes security between a web browser (server) and a website (client). It is like a tunnel that ensures that information travels from one to the other without the risk of it being intercepted by outside parties. SSL ensures that confidential information remains private when transmitted. For safety measures, encrypt your connections with this security protocol.
- **Don't overcomplicate your network:** A complex network is more likely to collapse than a simpler one because of all the unnecessary services and devices associated with it. As much as possible, keep your infrastructure simple. If, for example, you have a wireless connection that you don't really understand the point of, just take it down. Unless it's a staple in your business, it's probably just making your network infrastructure weaker. Remember that most disasters happen through wireless communications. If you still decide that a wireless network will do you good, at least secure it properly so your whole infrastructure won't be compromised when things get out of hand.
- **Protect your network inside and out:** To avoid cyber incidents that involve security breach, secure your network from the inside out. Tools that monitor how your network is used by employees are not difficult to find or set up. Better address the problem before it occurs. Virus and malware protection software are also recommendable. Sometimes, employees can be careless in their transactions. A backup plan is indeed indispensable here. There are other ways for you to shield your network from both internal and external vulnerabilities. Make use of all of them.
- **Combat problems before they come:** As a businessman, you should be interested not only about your company's present network infrastructure. The future looms ahead, and it should also be one of your concerns. Create a security policy that underlines all the basic measures that you need to undertake to protect your network. Include even those points that are still unknown to you, especially in terms of network traffic. Define your perimeters and build a strategy that considers every possibility.

Securing your network infrastructure is not a one-time project. Yes, it has a definite start, but it never really ends. It's a process of building and maintaining that goes on and on as long as your business continues to carry forward. (PA)

## 21. Concept of VPN and IpSec

- A **virtual private network** (**VPN**) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across a VPN may therefore benefit from the functionality, security, and management of the private network.[1]
- VPN technology was developed to allow remote users and branch offices to securely access corporate applications and other resources. To ensure security, data would travel through secure tunnels and VPN users would use authentication methods – including passwords, tokens and other unique identification methods – to gain access to the VPN. In addition, Internet users may secure their transactions with a VPN, to circumvent geo-restrictions and censorship, or to connect to proxy servers to protect personal identity and location to stay anonymous on the Internet. However, some Internet sites block access to known VPN technology to prevent the circumvention of their geo-restrictions, and many VPN providers have been developing strategies to get around these roadblocks.

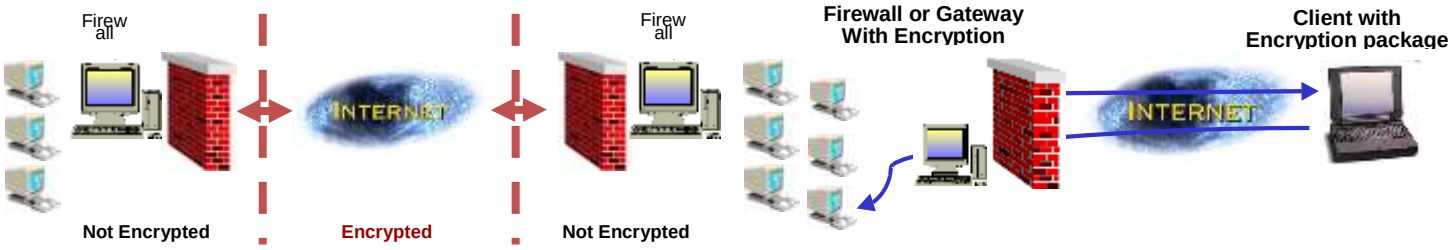
- A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN). From a user perspective, the resources available within the private network can be accessed remotely.

**VPN systems may be classified by:**

- the tunneling protocol used to tunnel the traffic
- the tunnel's termination point location, e.g., on the customer edge or network-provider edge
- the type of topology of connections, such as site-to-site or network-to-network
- the levels of security provided
- the OSI layer they present to the connecting network, such as Layer 2 circuits or Layer 3 network connectivity
- the number of simultaneous connections.

**Types of VPN**

1. **Firewall-to-Firewall VPN**
   - Data is encrypted when it leaves Firewall #1 and crosses the Internet
   - The data is authenticated and decrypted when it reaches Firewall #2.
2. **Client-to-Firewall VPN**




**IPSec**

IPsec, also known as the Internet Protocol Security or IP Security protocol, defines the architecture for security services for IP network traffic. IPsec describes the framework for providing security at the IP layer, as well as the suite of protocols designed to provide that security, through authentication and encryption of IP network packets. Also included in IPsec are protocols that define the cryptographic algorithms used to encrypt, decrypt and authenticate packets, as well as the protocols needed for secure key exchange and key management.

The most important protocols considered a part of IPsec include:

- The IP Authentication Header (AH), specified in RFC 4302, defines an optional packet header to be used to guarantee connectionless integrity and data origin authentication for IP packets, and to protect against replays.
- The IP Encapsulating Security Payload (ESP), specified in RFC 4303, defines an optional packet header that can be used to provide confidentiality through encryption of the packet, as well as integrity protection, data origin authentication, access control and optional protection against replays or traffic analysis.
- Internet Key Exchange (IKE), defined in RFC 7296, "Internet Key Exchange Protocol Version 2 (IKEv2)," is a protocol defined to allow hosts to specify which services are to be incorporated in packets, which cryptographic algorithms will be used to provide those services, and a mechanism for sharing the keys used with those cryptographic algorithms.
- Previously defined on its own, the Internet Security Association and Key Management Protocol (ISAKMP) is now specified as part of the IKE protocol specification. ISAKMP defines how Security Associations (SAs) are set up and used to define direct connections between two hosts that are using IPsec. Each SA defines a connection, in one direction, from one host to another; a pair of hosts would be defined by two SAs. The SA includes all relevant attributes of the connection, including the cryptographic algorithm being used, the IPsec mode being used, encryption key and any other parameters related to the transmission of data over the connection.

**IPSec Modes**

- ***Transport Mode*** **–** protects only the payload portion of sent IP packet (I.e. not the header)
  When two individual hosts set up a directly connected IPsec VPN connection, the circuit can be said to be an example of a transport mode IPsec circuit. For example, a transport mode IPsec circuit might be set up to allow a remote IT support technician to log in to a remote server to do maintenance work. Transport mode IPsec is used in cases where one host needs to interact with another host; the two hosts negotiate the IPsec circuit directly with each other, and the circuit is usually torn down after the session is complete.
- **Tunnel Mode** – protects the entire header and payload of the packet

Usually used between secured network gateways, IPsec tunnel mode enables hosts behind one of the gateways to communicate securely with hosts behind the other gateway. For example, any users of systems in an enterprise branch office can securely connect with any systems in the main office if the branch office and main office have secure gateways to act as IPsec proxies for hosts within the respective offices. The IPsec tunnel is established between the two gateway hosts, but the tunnel itself can carry traffic from any hosts inside the protected networks. Tunnel mode is useful for setting up a mechanism for protecting all traffic between two networks, from disparate hosts on either end.


## 22. Business Continuity Planning (BCP) and its phases

Business continuity planning (or business continuity and resiliency planning) is the process of creating systems of prevention and recovery to deal with potential threats to a company.

A business continuity plan (BCP) is a plan to help ensure that business processes can continue during a time of emergency or disaster. Such emergencies or disasters might include a fire or any other case where business is not able to occur under normal conditions. Businesses need to look at all such potential threats and devise BCPs to ensure continued operations should the threat become a reality.

A business continuity plan involves the following:

1. Analysis of organizational threats
2. A list of the primary tasks required to keep the organization operations flowing
3. Easily located management contact information
4. Explanation of where personnel should go if there is a disastrous event
5. Information on data backups and organization site backup
6. Collaboration among all facets of the organization
7. Buy-in from everyone in the organization

### BCP phases

1. Project management & initiation
2. Business Impact Analysis (BIA)
3. Recovery strategies
4. Plan design & development
5. Testing, maintenance, awareness, training

### I - Project management & initiation

- Establish need (risk analysis)
- Get management support
- Establish team (functional, technical, BCC - Business Continuity Coordinator)
- Create work plan (scope, goals, methods, timeline)
- Initial report to management
- Obtain management approval to proceed

### II - Business Impact Analysis (BIA)

- Goal: obtain formal agreement with senior management on the MTD for each time-critical business resource
- MTD - maximum tolerable downtime, also known as MAO (Maximum Allowable Outage)
- Quantifies loss due to business outage (financial, extra cost of recovery, embarrassment)
- Does not estimate the probability of kinds of incidents, only quantifies the consequences

### BIA phases

- Choose information gathering methods (surveys, interviews, software tools)
- Select interviewees
- Customize questionnaire
- Analyze information

- Identify time-critical business functions
- Assign MTDs
- Rank critical business functions by MTDs
- Report recovery options
- Obtain management approval

**III - Recovery strategies**

- Recovery strategies are based on MTDs
- Predefined
- Management-approved
- Different technical strategies
- Different costs and benefits
- How to choose?
- Careful cost-benefit analysis
- Driven by business requirements
- Strategies should address recovery of:
    - Business operations
    - Facilities & supplies
    - Users (workers and end-users)
    - Network, data center, telecommunications (technical)
    - Data (off-site backups of data and applications)

**IV - BCP development / implementation**

- Detailed plan for recovery
    - Business & service recovery plans
    - Maintenance
    - Awareness & training
    - Testing
- Sample plan phases
    - Initial disaster response
    - Resume critical business operations
    - Resume non-critical business operations
    - Restoration (return to primary site)
    - Interacting with external groups (customers, media, emergency responders)

**V - BCP final phase**

- Testing
    - Until it's tested, you don't have a plan
    - Testing types: Structured walk-through, Checklist, Simulation, Parallel, Full interruption.
- Maintenance
    - Fix problems found in testing
    - Implement change management
    - Audit and address audit findings
- Awareness / Training
    - BCP team is probably the DR team
    - BCP training must be on-going, part of corporate culture

## 23. Disaster Types

**Natural**

- Thunderstorms
- Tornadoes
- Lightning

- Earthquakes
- Volcanoes
- Tsunami
- Landslides
- Floods, droughts
- Epidemics

**Anthropogenic, man-made**

- **Non-intentional**
  - Acts of people
  - Technological system failures
  - Hazardous materials
  - Environmental
  - Nuclear
  - Aviation, railways
  - Fires, collapse
- **Intentional**
  - Workplace violence
  - Civil disobedience
    - Labor riots
    - Political riots
  - Terrorism
  - Weapons of mass destruction

## 24. Disaster recovery Planning

- DR : The planned process of restoring systems, data, and infrastructure required to support key ongoing business operations.
- A DR plan : a proactive measure to minimize a company's downtime during sudden emergencies
- An unforeseen event : fire, flood, earthquake, etc
- A Disaster Recovery Plan (DRP) is a business plan that describes how work can be resumed quickly and effectively after a disaster. Disaster recovery planning is just part of business continuity planning and applied to aspects of an organization that rely on an IT infrastructure to function.
- The overall idea is to develop a plan that will allow the IT department to recover enough data and system functionality to allow a business or organization to operate - even possibly at a minimal level.
- The creation of a DRP begins with a DRP proposal to achieve upper level management support. Then a business impact analysis (BIA) is needed to determine which business functions are the most critical and the requirements to get the IT components of those functions operational again after a disaster, either on-site or off-site.
- Every employee must be made aware of the DRP and when implemented, effective communication is essential. The DRP must include a comprehensive off-site data backup and an on/off-site recovery plan.
- The biggest issue may be the sourcing of an alternate location with adequate equipment, but there are many places where data center time and bandwidth can be rented so these arrangements could also be included in a DRP. Some companies can operate from just a single server so a backup machine can be kept at a remote location and kept up to date with a regular backup of the essential data required to operate being made. This would suit a small organization, but where there are more computers and a data center involved there needs to be a more extensive plan made.
- A DRP may require employees to relocate to a hotsite to resume work, if work cannot be conducted at the normal business site. This hotsite is an off-site location supplied with the computer equipment and data necessary to continue an organization's normal work.
- It is imperative that organizations not only develop a DRP but also test it, train personnel and document it properly before a real disaster occurs. This is one reason why off-site hosting of all IT services can be a good choice for the protection they provide; in disaster situations personnel can access data easily from a new location, whereas relocating a terminally damaged data centre and getting it operational again is not an easy job.
- Often a specialized disaster recovery planning consultant is hired to assist organizations in attending to the many details that can arise during such contingency planning.

**The following key of Disaster Recovery Plan (DRP) should be to:**

- Provide for the safety and well-being of people on the premises at the time of a disaster;
- Continue critical business operations;

- Minimize the duration of a serious disruption to operations and resources (both information processing and other resources);
- Minimize immediate damage and losses;
- Establish management succession and emergency powers;
- Facilitate effective co-ordination of recovery tasks;
- Reduce the complexity of the recovery effort;
- Identify critical lines of business and supporting functions;

**What is the purpose of a Disaster Recovery Plan (DRP)?**

The primary purposes of a Disaster Recovery Plan (DRP) are as following:

1. **Prevention** (pre-disaster): The pre-planning required — using mirrored servers for mission critical systems, maintaining hot sites, training disaster recovery personnel – to minimize the overall impact of a disaster on systems and resources. This pre-planning also maximizes the ability of an organization to recover from a disaster.
2. **Continuity** (during a disaster): The process of maintaining core, mission-critical systems and resource "skeletons" (the bare minimum assets required to keep an organization in operational status) and/or initiating secondary hot sites during a disaster. Continuity measures prevent the whole organization from folding by preserving essential systems and resources.
2. **Recovery** (post-disaster): The steps required for the restoration of all systems and resources to full, normal operational status. Organizations can cut down on recovery time by subscribing to quick-ship programs (third-party service providers

**Difference between BCP and DRP**

- Technically the Business Continuity Plan (BCP) refers to the means by which loss of business may be avoided and it ought to define the business requirements for continuity of operations. It defines the business requirements for a Disaster Recovery Plan (DRP).
- Technically, the Disaster Recovery Plan (DRP) deals with the restoration of computer systems with all attendant software and connections to full functionality under a variety of damaging or interfering external conditions. In daily practice Business Continuity often refers to disaster recovery from a business point-of-view, or dealing with simple daily issues, such as a failed disk, failed server or database, possibly a bad communications line. It is often referred to as the measure of lost time in an application, possibly a mission critical application.
- In daily practice Disaster Recovery often refers to major disruption, such as a flooded building, fire or earthquake disrupting an entire installation. The issue of Business Continuity certainly arises when Disaster Recovery is required.
- In short we can say that Disaster Recovery Plans addresses the procedures to be followed during and after the loss whereas BCP is the preventive process put in place in preparation for the handling of a disaster

## 25. Concept of RTO and RPO

There is a good chance that you would like to see your business survive any future disaster, and any problems that follow as well. While it is nearly impossible to predict what the next disaster will be, it's easy to prepare for, especially if you have an effective business continuity plan. When it comes to these plans, there are many key metrics you need to be aware of and the most important two are RTO and RPO.

While both RTO and RPO are important elements of continuity plans, and they both sound fairly similar, they are actually quite different. In this article we define RTO and RPO and take a look at what the difference is between the two concepts.

***RTO defined***

RTO, or Recovery Time Objective, is the target time you set for the recovery of your IT and business activities after a disaster has struck. The goal here is to calculate how quickly you need to recover, which can then dictate the type or preparations you need to implement and the overall budget you should assign to business continuity.

If, for example, you find that your RTO is five hours, meaning your business can survive with systems down for this amount of time, then you will need to ensure a high level of preparation and a higher budget to ensure that systems can be recovered quickly. On the other hand, if the RTO is two weeks, then you can probably budget less and invest in less advanced solutions.

***RPO defined***

RPO, or Recovery Point Objective, is focused on data and your company's loss tolerance in relation to your data. RPO is determined by looking at the time between data backups and the amount of data that could be lost in between backups.

As part of business continuity planning, you need to figure out how long you can afford to operate without that data before the business suffers. A good example of setting an RPO is to imaging that you are writing an important, yet lengthy, report. Think to yourself that eventually your computer will crash and the content written after your last save will be lost. How much time can you tolerate having to try to recover, or rewrite that missing content?

That time becomes your RPO, and should become the indicator of how often you back your data up, or in this case save your work. If you find that your business can survive three to four days in between backups, then the RPO would be three days (the shortest time between backups).

***What's the main difference between RTO and RPO?***

The major difference between these two metrics is their purpose. The RTO is usually large scale, and looks at your whole business and systems involved. RPO focuses just on data and your company's overall resilience to the loss of it.

While they may be different, you should consider both metrics when looking to develop an effective BCP. If you are looking to improve or even set your RTO and RPO, contact us today to see how our business continuity systems and solutions can help.

## 26. Electronic Transaction Act ( Focus on Cyber Crime)

Government of Nepal has enacted Electronic Transaction Act 2063 to control cyber crimes The first cyber crime in the world is registered to be occurred at 1820 at France. The rule and acts are listed below with penalty ranges:

- Act 48: Destroying Secrecy: Up to Rs 100000 or 2 years imprisonment
- Act 49: False Information Providing: Rs 100000 or 2 yrs
- Act 52: Computer Conspiracy: Rs 100000 or 2 year
- Act 52: Not registering Recommended Information or document: Up to Rs 50000
- Act 44: Computer source code theft, destruction or changing: 3 year Imprisonment or Up to 200000 fine or both
- Act 45: Unauthenticated approach on computer devices: Rs 200000 or 3 year prison or both
- Act 47: Publishing illegal things in any electronic form: Rs 100000 fine or 5 yrs prison or both

## 27. Ethics in Information Security adhered by Professional Organizations

- Laws: rules that mandate or prohibit certain behavior in society; drawn from ethics
- Ethics: define socially acceptable behaviors; based on cultural mores (fixed moral attitudes or customs of a particular group)
- Many organizations have codes of conduct and/or codes of ethics
- Organization increases liability if it refuses to take measures known as due care
- Due diligence requires that organization make valid effort to protect others and continually maintain that effort

**Ethical Concepts In Information Security**

1) Thou shalt not use a computer to harm other people.
2) Thou shalt not interfere with other people's computer work.
3) Thou shalt not snoop around in other people's computer files.
4) Thou shalt not use a computer to steal.
5) Thou shalt not use a computer to bear false witness.
6) Thou shalt not copy or use proprietary software for which you have not paid.
7) Thou shalt not use other people's computer resources without authorization or proper compensation.
8) Thou shalt not appropriate other people's intellectual output.
9) Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10) Thou shalt always use a computer in ways that insure consideration and respect for your fellow humans."

## 28. IS Audit Process

**Audit is** "Systematic process by which a qualified, competent, independent team or person objectively obtains and evaluates evidence regarding assertions about a process for the purpose of forming an opinion about and reporting on the degree to which the assertion is implemented." IS=specific definition for audit and Control = method of security defense

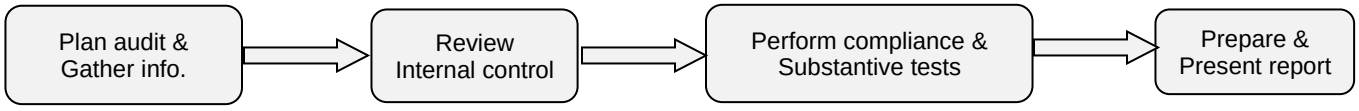



**Fig. Simplified Audit Process**

IS Audit: Any audit that wholly or partially evaluates automated information processing system, related non-automated processes, & their interfaces

(i) Step 1: Plan the audit (auditor)
(ii) Step 2: Hold audit kickoff meeting (auditor/orga nization)
(iii) Step 3: Gather data and test IT controls (auditor/organization)
(iv) Step 4: Remediate identified deficiencies (organization)
(v) Step 5: Test remediated controls (auditor/organization)
(vi) Step 6: Analyze and report findings (auditor)
(vii) Step 7: Respond to findings (organization)
(viii) Step 8: Issue final report (auditor)

## 29. Penetration testing

- Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.
- Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.
- The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents.
- Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in.

**Pen test strategies include:**

- **Targeted testing**: Targeted testing is performed by the organization's IT team and the penetration testing team working together. It's sometimes referred to as a "lights-turned-on" approach because everyone can see the test being carried out.
- **External testing**: This type of pen test targets a company's externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access.
- **Internal testing:** This test mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause.
- **Blind testing:** A blind test strategy simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team that's performing the test beforehand. Typically, they may only be given the name of the company. Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive.
- **Double blind testing:** Double blind testing takes the blind test and carries it a step further. In this type of pen test, only one or two people within the organization might be aware a test is being conducted. Double-blind tests can be useful for testing an organization's security monitoring and incident identification as well as its response procedures.

**Methods and Techniques of PT**

1) Black box: zero-knowledge testing
2) White Box: complete-knowledge testing
3) Gray Box: tester simulates an inside employee.

**Stages of PT**

- Scope/Goal Definition
- Information Gathering
- Vulnerability Detection
- Information Analysis and Planning.
- Attack& Penetration/Privilege Escalation.
- Result Analysis & Reporting.
- Cleanup.