Unit IV

CHAPTER 4

Intrusion Detection System

Syllabus Topic : Intrusion Detection System : Concepts, Detection Models, IDS Features

4.1 Intrusion Detection Systems

Q. 4.1.1 Write short note on IDS. (Ref. Sec. 4.1) (5 Marks)

Intrusion Detection Systems plays an important like the firewall because they help us to detect the type of attack that is being done to our system and then to make a solution to block them. It also does monitoring part like tracing logs, looking for doubtful signatures and keeping history of the events triggered. They help us to check the connection integrity and authenticity that occur.

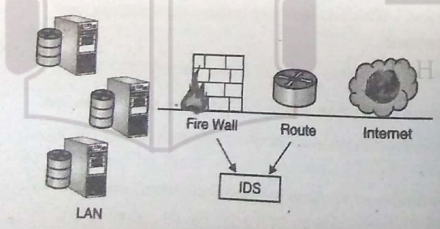

Fig. 4.1.1

4.1.1 Intrusion Detection Tools

There are many IDS tools; one of the best intrusion detection tool is **Snort**. It is software based, but is an open source so it is free and also easy to configure. It has a real time signature based network – IDS, which notifies the system administrators or attacks like port scanners, DDOS attacks, CGI attacks, backdoors, OS finger printing.

Following things can be used as IDS :

- Black ICE Defender.
- Cyber Cop Monitor.
- Check point Real Secure.
- Cisco Secure IDS.
- Vanguard Enforcer.
- Lucent Real Secure.

Syllabus Topic : IDS Types

4.1.2 Types of IDS

Q. 4.1.2 What are the different types of IDS? (Ref. Sec. 4.1.2) (5 Marks)

There are mainly three types of IDS used in networks they are as follows:

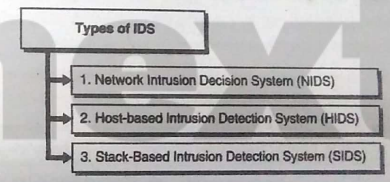

Fig. 4.1.2 : Total of IDS

1. Network Intrusion Decision System (NIDS)

It is an independent platform that identifies intrusions by examining network traffic and monitors multiple hosts, which was developed in 1986 by Pete R. Network intrusion detection systems gain access to network traffic by connecting to a network hub, network switch configured for port mirroring, or network tap. In a NIDS, sensors are located at choke points in the network to be monitored, often in the demilitarized zone (DMZ) or at network borders. Sensors capture all network traffic and analyze the content of individual packets for malicious traffic. An example of a NIDS is Snort.

2. Host-based Intrusion Detection System (HIDS)

It consists of an agent on a host that identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability databases,

Access control lists, etc.) and other host activities and state. In a HIDS, sensors usually consist of a software agent. Some application-based IDS are also part of this category. Examples of HIDS are Tripwire and OSSEC.

➜ **3. Stack-based Intrusion Detection System (SIDS)**

This type of system consists of an evolution to the HIDS systems. The packets are examined as they go through the TCP/IP stack and, therefore, it is not necessary for them to work with the network interface in promiscuous mode. This fact makes its implementation to be dependent on the Operating System that is being used. Intrusion detection systems can also be system-specific using custom tools and honeypots.

4.2 Passive and Reactive Systems

- In a passive system, the Intrusion Detection System (IDS) sensor detects a potential security breach, logs the information and signals an alert on the console and/or owner.
- In a reactive system, also known as an Intrusion Prevention System (IPS), the IPS auto-responds to the suspicious activity by resetting the connection or by reprogramming the firewall to block network traffic from the suspected malicious source.
- The term IDPS is commonly used where this can happen automatically or at the command of an operator; systems that both "detect (alert)" and "prevent".

Syllabus Topic : Intrusion Prevention Systems

4.2.1 Intrusion Prevention Systems

Q.4.2.1 Write short note on IPS. (Ref. Sec. 4.2.1) (5 Marks)

- Intrusion Prevention Systems (IPS), also known as Intrusion Detection and Prevention Systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity.
- The main functions of intrusion prevention systems are to identify malicious activity, log information about said activity, attempt to block/stop activity, and report activity.
- Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity.
- The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected.

- More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address.
- An IPS can also correct Cyclic Redundancy Check (CRC) errors, un-fragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options.

4.2.2 Detection Methods

Q. 4.2.2 What are the different detection methods? (Ref. Sec. 4.2.2) (5 Marks)

- The majority of intrusion prevention systems utilize one of three detection methods: signature-based, statistical anomaly-based and stateful protocol analysis.

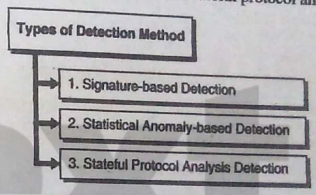

Fig. 4.2.1 : Types of Detection method

➜ **1. Signature-based detection**

- This method of detection utilizes signatures, which are attack patterns that are preconfigured and predetermined. A signature-based intrusion prevention system monitors the network traffic for matches to these signatures.
- Once a match is found the intrusion prevention system takes the appropriate action. Signatures can be exploit-based or vulnerability-based.
- Exploit-based signatures analyze patterns appearing in exploits being protected against, while vulnerability-based signatures analyze vulnerabilities in a program, its execution, and conditions needed to exploit said vulnerability.

➜ **2. Statistical anomaly-based detection**

- This method of detection baselines performance of average network traffic conditions.

- After a baseline is created, the system intermittently samples network traffic, using statistical analysis to compare the sample to the set baseline. If the activity is outside the baseline parameters, the intrusion prevention system takes the appropriate action.

➜ **3. Stateful protocol analysis detection**

- This method identifies deviations of protocol states by comparing observed events with "predetermined profiles of generally accepted definitions of benign activity."
- Event Management ensures that all CIs are constantly monitored and define a process to categorize these events so that appropriate action can be taken if required.
- IT Operation Manager is the process owner of this process.

Event management can be applied on the following aspects :

1. Configuration Items (CIs).
2. Security.
3. Environment Conditions (e.g. fire and smoke detections).
4. Normal activity (e.g. tracking the use of an application or performance of a server)

Software licence monitoring for usage to ensure legal licence utilization and allocation

There are two types of monitoring tools as described below :

1. Active monitoring tools monitor CIs for their status and availability. Any deviation from normal operation is communicated the appropriate team for action
2. Passive monitoring tools detect and correlate operational alerts or communications generated by CIs.

Syllabus Topic : IDS Deployment Considerations

4.2.3 IDS Deployment Considerations

Q. 4.2.3 Write a short note on IDS deployment consideration.(Ref. Sec. 4.2.3) (5 Marks)

- Installing a Network IDS (NIDS) onto a network requires a significant amount of thought and planning. In addition to the technical issues and product selection there are resource issues, from product cost to manning the sensor feeds and supporting the infrastructure that must also be considered.
- The scope of this article considers the worst case scenario, that of deploying a NIDS on a remote network (target). The introduction of an IDS into a organization's network can be sensitive and often has political implications with the network staff, and thus a checklist written from the perspective of an outside consultant (even if the IDS is deployed internally) that appeases all parties can be useful to ensure a successful implementation.
- When installing an IDS a policy needs to be developed to ensure responsibilities are clearly defined. This is especially important when delivering an IDS capability remotely or to another organisation's network. The Junction of Maintenance (JoM) defines where your responsibility for the hardware starts and finishes, and this will usually be the network switch port or tap with which the IDS connects to the target network.
- On the subject of failing hardware, people administering the target network must be made fully aware that if network taps are used, even fail safe taps can take upto a second for the interfaces to re-negotiate and could potentially disrupt services, though recent improvements have reduced this latency considerably.
- If the network is remote then it is advisable for the policy to reflect that the target network manpower can be called upon for a predefined duration for power resets, etc. Attempting this retrospectively through contractual alteration, if required, can be expensive and time consuming. If you rely on the distant network for support, ensure you have a telephone authentication system in place and don't fall victim to a social engineering attack. It's all too easy for an attacker or Pen Tester to call the local staff where your IDS is installed and ask them to power it down.
- Most of these issues can be avoided if you are willing to have your IDS application reside on one of the target network's hosts, though in my experience it can never be completely trusted and raises the question of who maintains the software and OS deployed on the system.
- If an OS update corrupts the IDS application, then who takes responsibility for fixing it? Finally, discuss and set in policy the rules of engagement for automated response. This is especially important when you are deploying Intrusion Prevention Systems.

4.2.4 Comparing IPS versus IDS

Q. 4.2.4 Differentiate between IPS and IDS. (5 Marks)

- An Intrusion Prevention System or inline IDS will block packets that meet the criteria of an event signature. These packets could have legitimately been accepted by the firewall and allowed through. As signatures can block packets in a fashion similar to a firewall, there are some that advocate replacing firewalls with IPS. I feel this is a dangerous step. In my opinion an IPS complements the firewall very well and they work well together, but the firewall should be left in place.

- This is a good time to mention the dreaded false positives. The myth that an IPS will kill a network through its false positives doesn't have to hold true. It can be set to simply alert rather than block, thus only blocking those packets where the likelihood of a false positive is very low. An IDS can work in a similar fashion to an IPS, though.
- Rather than blocking packets in line, it can craft various responses: TCP resets to the source or destination (or in some cases both) of the offending packet, crafting unreachable/unauthorized replies and spoofing the border device. A big seller for stateful IPS is preventing the leaking of confidential information from an organisation. For example, you might want to retain corporate knowledge by blocking any document that contains the word "prototype", from leaving the network through the use of an IPS signature.
- If the site has a policy for accepted use at their gateways, it is essential to use this to build the policy for your IDS. For instance, there is little point in reporting POP3 usage if it is permitted. There is some value in recommending changes to policies if they are blatantly insecure, but be careful not to oversell the issue and alienate the other network staff. At this stage your priority is to simply get the IDS or IPS in the door. Once the IDS starts chattering you can revisit those "practises dangerous to security".
- Policy also needs to be defined regarding how you respond to an incident and should include statements that direct forensics and evidence preservation activities. Furthermore, what assistance can you expect to receive from the site itself following an incident and what actions are they expecting you to complete?

4.2.5 Gaining IDS Mindshare

- Gaining the trust of the target network's staff is imperative to a successful installation. I always find that the target network sys admin's concerns regarding intrusion detections are not necessarily focused on external traffic gaining access to their network, but what you will see of their poor practices and, more importantly, how you will react. I find that an amnesty of a predetermined duration, say a month, is a great icebreaker, where all detections are discussed with sys admins before their escalation.
- Possible exceptions to this must be discussed or you may destroy any trust, such as with high risk intrusions that occur out of office hours and detections of such a nature that they must be reported to the authorities under duty of care (i.e., discovering paedophilia). Winning the hearts and minds of all network staff will pay dividends when it comes to reducing false positives, post install.

4.2.6 Gather Network Topology Diagrams

- The availability of up-to-date network diagrams is essential not only for locating the best site for an IDS, but also post installation.
- The IDS analysts must be able to understand the events that they are seeing and how they relate to the network. They should include: network devices, bandwidth, transmission media, IP addresses, sub-netting information, default gateways, operating systems, host names, applications, and more.
- Be prepared to create them yourself as many of the diagrams out there are no more than scribbles on the back of a cigarette packet. Whilst you are making enquiries, ask if there are any planned upgrades over the next 12 months which may affect your choice of sensor, especially bandwidth (replacing a 100mb sensor for a Gigabyte sensor could be very costly if it is only six months down the line).

4.2.7 Identify Physical Infrastructure

- You have to identify your requirements for the installation such as rack space, switch/hub ports, power outlets, UPS, cooling, taps and any mandatory local requirements like fiber infrastructure and fail over. Where you reserve any of the above for your use it is best to label them, otherwise rest assured, they will be gone when it comes to installation day.
- Get/make diagrams of everything: rack layouts, room layouts, building layouts, etc. I can't stress this enough, staff move on and it's all too easy to lose your IDS in a large data warehouse. Identify telephones close to where the IDS will be located, which is great for remote reboots. I asked one IDS vendor to include a feature that allows me to blink all the lights on the front of the box when I wanted distant users to reboot; this was after some bright spark cycled the power on the firewall by mistake.
- HP has a great solution for remote access with the "Lights-Out" card on their DL servers. This great device then gives you full KVM into the machine so you can do all the normal KVM things from the other side of the world. In addition you can power up from off, even adjust BIOS settings. All that is required is another power socket and an extra IP address.

4.2.8 Sensor Topology Discussion

Some considerations need to be made when installing your IDS :

1. NIPS or NIDS	2. Method of Connection
3. Site Access	4. Network Name
5. Network Function	6. Target date
7. Points of contact	

➜ **1. NIPS or NIDS**

- As discussed earlier, this depends on your requirements. My preference is for NIPS though configured to be fully open and not blocking.

➜ **2. Method of Connection**

- Do you use taps or the span port on a switch? Obviously a NIPS must be inline, though I have seen an IPS tap which supports a backup IPS should the first fail. The tap is configurable to fail open or fail closed. The sensor will need to be installed either in a rack or a desktop PC, depending on the deployed infrastructure. Will you need rack shelving and will your equipment be too deep for the racks?
- Management. You need to decide whether you manage your IDS Inband, Outband or Pseudo Outband.

➜ **3 Site Access**

- If this is a remote installation, are there any restrictions in accessing the site? Further, if you are not employed by the target organization, will your staff need to be cleared before arrival?

➜ **4. Network Name**

- This is self explanatory but essential when dealing with large data centres.

➜ **5. Network Function**

- This is useful for the analysts when responding to an incident.

➜ **6. Target date**

- When is it convenient to install the IDS? If downtime is required this will likely need to be provisioned in advance. Will the install have to be outside of normal hours?

➜ **7. Points of contact**

- Identify all key players from network staff to security staff, both network and physical, and have them listed in one place in case of a major incident.

4.2.9 Pre- Installation Phase

☞ **Procurement**

- It should go without saying, but shipping delays can occur that setback the installation.
- Ensure you procure the equipment well in advance, and on arrival lock it away.

☞ **Quarantine**

- Delays often occur, therefore once the sensor is built put it somewhere safe, well away from those well-intentioned "borrowers".
- I like to place mine in an IDS crèche, all connected up, where it can report to a manager, receive updates and be soak tested, and best of all nobody can "borrow" any bits unnoticed.

☞ **Building**

- When you build an IDS/IPS think secure install at all times.
- Harden it as much as possible as there is nothing worse for your credibility than having an IDS rooted.

☞ **Testing**

- It is useful to soak test an IDS before deployment, ideally in the same configuration as you will use on site. Make sure you test any taps for failing in the correct manner, either open or closed. If possible, fluctuate temperature and place the IDS under considerable network load (warm it up).
- Ensure your own router, firewalls and VPN permit access from the remote network; perform simulated remote updates to the IDS and operating system.

☞ **Installing the sensor**

- If all the above has gone according to plan, the installation should be a dream. Whilst you are still onsite, it is probably worth investigating the initial events with the site admins.
- If a third party has installed the IDS try to call the site ASAP to clear off those initial (often many) false positives. Do not try to make assumptions. The site sys admins are the experts on their network and should be able to provide the technical feedback to those first few events.

Post Installation feedback

- False positive tuning is essential. The first coarse tuning should have occurred by using the site's policy to define the initial IDS policy. Subsequent fine tuning should be carried out periodically. Rather than attempting this on an event-by-event basis, wait a week and look at the historical information, sorted by count.
- Rather than adjust the IDS policy to reduce false positives, I find it easier to try and cure the source of the alert, which will require some site interaction. For instance, if you see alerts for SNMP "public" community string ask the site to change away from the default rather than ignore the event. You will need to provide as much information about each false positive as you can in a tabular form and also, if possible, suggest a course of action to the administrators for tuning/patching the relevant system.
- If this course of action cannot be completed then you will have to take IIDS tuning action, which could include filtering the source or destination address, removing the signature entirely or reducing it's severity.
- All tuning needs to be fully documented, and do not forget to ensure that there is a column in the documentation for the regular network staff to comment on your recommendations.
- The second false positive reduction period should occur at around the one month stage. After this point the IDS should be singing sweetly (depending upon your choice of IDS) and false positives could be dealt with on an individual basis.

Syllabus Topic : Security Information and Event Management (SIEM)

4.3 Security Information and Event Management (SIEM)

Q. 4.3.1 Write short note on Security Information and Event Management. (Ref. Sec. 4.3) (5 Marks)

- Security Information and Event Management (SIEM) is an approach to security management that combines SIM (Security Information Management) and SEM (Security Event Management) functions into one security management system. The acronym SIEM is pronounced "sim" with a silent e.
- The underlying principles of every SIEM system is to aggregate relevant data from multiple sources identify deviations from the norm and take appropriate action. For

example, when a potential issue is detected, a SIEM might log additional information, generate an alert and instruct other security controls to stop an activity's progress.

- At the most basic level, a SIEM system can be rules-based or employ a statistical correlation engine to establish relationships between event log entries. Advanced SIEMs have evolved to include User and Entity Behavior Analytics (UEBA) and Security Orchestration and Automated Response (SOAR).
- Payment Card Industry Data Security Standard (PCI DSS) compliance originally drove SIEM adoption in large enterprises, but concerns over Advanced Persistent Threats (APTs) have led smaller organizations to look at the benefits a SIEM Managed Security Service Provider (MSSP) can offer.
- Being able to look at all security-related data from a single point of view makes it easier for organizations of all sizes to spot patterns that are out of the ordinary.
- Today, most SIEM systems work by deploying multiple collection agents in a hierarchical manner to gather security-related events from end-user devices, servers, network equipment, as well as specialized security equipment like firewalls, antivirus or intrusion prevention systems.
- The collectors forward events to a centralized management console where security analysts sift through the noise, connecting the dots and prioritizing security incidents.
- In some systems, pre-processing may happen at edge collectors, with only certain events being passed through to a centralized management node. In this way, the volume of information being communicated and stored can be reduced.
- Although advancements in machine learning are helping systems to flag anomalies more accurately, analysts must still provide feedback, continuously educating the system about the environment.
- Here are some of the most important features to review when evaluating SIEM products:
  1. **Integration with other controls :** Can the system give commands to other enterprise security controls to prevent or stop attacks in progress ?
  2. **Artificial intelligence :** Can the system improve its own accuracy by through machine and deep learning?
  3. **Threat intelligence feeds :** Can the system support threat intelligence feeds of the organization's choosing or is it mandated to use a particular feed ?
  4. **Robust compliance reporting :** Does the system include built-in reports for common compliance needs and the provide the organization with the ability to customize or create new compliance reports ?

5. **Forensics capabilities :** Can the system capture additional information about security events by recording the headers and contents of packets of interest ?

Syllabus Topic : Voice over IP (VoIP) : Background

4.4 VoIP

Q. 4.4.1 What is VoIP? Explain VoIP protocols. (Ref. Sec. 4.4) (5 Marks)

- VoIP is the acronym for Voice over Internet Protocol. It means telephone services over Internet. Traditionally Internet had been used for exchanging messages but due to advancement in technology, its service quality has increased manifold.

Fig. 4.4.1

- It is now possible to deliver voice communication over IP networks by converting voice data into packets. VoIP is a set of protocols and systems developed to provide this service seamlessly.
- There are some of the protocols used for VoIP :
  - H.323
  - Session Initiation Protocol (SIP)
  - Session Description Protocol (SDP)
  - Media Gateway Control Protocol (MGCP)
  - Real-time Transport Protocol (RTP)
  - Skype Protocol

H.323

H.323 is a VoIP standard for defining the components, protocols and procedures to provide real-time multimedia sessions including audio, video and data transmissions over packet switched networks. Some of the services facilitated by H.323 include :

- **IP telephony**
- **Video telephony**

  Simultaneous audio, video and data communications
- **SIP**

- SIP is an acronym for Session Initiation Protocol. SIP is a protocol to establish, modify and terminate multimedia sessions like IP telephony. All systems that need multimedia sessions are registered and provided SIP address, much like IP address. Using this address, caller can check callee's availability and invite it for a VoIP session accordingly.
- SIP facilitates multiparty multimedia sessions like video conferencing involving three or more people. In a short span of time SIP has become integral to VoIP and largely replaced H.323.

Syllabus Topic : VoIP Components

4.4.1 VoIP Components

Q. 4.4.2 What are the components of VoIP? (Ref. Sec. 4.4.1) (5 Marks)

The four most important VoIP components are :

1. Signaling Gateway Controller
2. Media Gateway
3. Media Server
4. Application Server

1. Signaling Gateway Controller

As you might remember from my VoIP Essentials article, the Signaling Gateway Controller (SGC) is known as a "called agent" because of its call control function and is also commonly referred to as a "Media Gateway Controller" because of its Media Gateway control function.

The SGC entity has multiple roles. It is the heart of VoIP platform; its main role is to connect the PSTN (Public Switched Telephone Network) world with the IP world. To simplify, the main characteristics of the SGC component are :

- **Support of Signaling System 7 (SS7) protocol stack** which is the PSTN world's main Signaling protocol suite (sometimes a separate entity called Signaling Gateway is used for this exact purpose).
- Full support of voice call control protocols such as H.323 or SIP which are purely IP signaling protocols.
- **Full support of media control protocols such as MGCP or Megaco (H.248)**which are used for controlling Media Gateway session connections and parameters.
- **Generate Call Detailed Records (CDRs)** for billing purposes.
- **Provide bandwidth management control through admission control mechanisms**, in other words, new sessions are admitted only if the system is able in terms of bandwidth to provide acceptable service to them.
- ***Support of bandwidth policing mechanisms*** with the use of media flow profiles, the Signaling Gateway Controller instructs the Media Gateway to monitor the RTP media flow and apply rate limit policies to aggressive flows. This mechanism also preserves appropriate Quality of Service levels.
- **Provisioning media connection** allocating media connection characteristics such as coding and packetization to Media Gateways as well as specific DS0 allocation for the reservation of Media resources.

As you can see, the SGC is the most important component of the whole VoIP structure, therefore, it has to be redundant. Hardware or software malfunction of this component is not tolerant. Also due to it's multitask and multiprocess behavior, it must be powerful in terms of CPU and memory.

➜ 2. Media Gateway

The Media Gateway's main role is the transmission of voice packets using the RTP transmission protocol. When the media gateway is used in a converged PSTN/IP network it has extra functions to perform such as packetization, since it uses TDM trunks from the one side and IP trunks on the other.

Let's examine the Media Gateway's main functions :

- **Support of MGCP or MEGACO** for call control under the administration of the Media Gateway Controller.

- **Transmission of Voice data using RTP** packetization of data is also applied when TDM trunks are interfacing the Media Gateway.
- **Support of T1/E1 trunks** for transferring voice in SS7 networks.
- **Support of different Compression algorithms** for fulfilling the requirements of the call as instructed by the SGC.
- **Manage Digital Signal Processing (DSP)** resources for ideal service offering.

Some sort of high availability can also be achieved by maintaining redundant IP links. The capabilities of the Media Gateway in terms of concurrent call support, mainly depends on the capacity of onboard DSPs and also the selection of codecs since different codecs have different processing requirements.

➜ 3. Media Server

A Media Server is used where added features are needed such as voicemail or video conferencing. Moreover, a media server is used when special tones or announcements need to be transmitted. Therefore, the media server has an important role within the VoIP architecture.

The main functions of the Media Server are :

- **Transmission of call progress** tones and special service announcements.
- **Voicemail functionality.**
- **Voice activated dialing.**
- **Voicemail to email transmission** voicemail can be transmitted as attachment to an email address.
- **Support for Interactive Voice Response (IVR)** call routing or even service activation can be performed based on dialed DTMF digits. The caller according to voice menus selects the appropriate DTMF digit that triggers the required service.

The Media Server is mainly controlled by an Application Server using SIP or pure XML. For the proper transmission of IVR, tone and announcement media proper IP routing towards the Media Gateway should exist.

➜ 4. Application Server

The major responsibility of an Application Server is to provide value-added services to the IP network. Global and customer specific services are provisioned here. Call characteristics and session specifications are influenced by the application server.

The main functions of the Application Server component are :

- **Support of customized private dialing plans.**
- **Basic service** offering basic services such as call forward always, call forward on busy, call waiting, call transfer, call park and voicemail are offered though the Application Server.
- **Advance service offering** advanced features such as call authorization using PIN, remote office, "follow me" plans can be offered by this component.
- **Generation of Call Detailed Records (CDRs)**
- **Free Phone Service** support of 800 number service where charging is applied to the called party.

The Application Server is the brain of the VoIP architecture. It communicates with the Signaling Gateway Controller through protocols such as H.323 or SIP. Services are implemented here and allocated to customers.

It is very important to have high availability configuration; you cannot tolerate service interruption in any way.

Syllabus Topic : VoIP Vulnerabilities and Countermeasures

4.4.2 VoIP Vulnerabilities and Countermeasures

Q. 4.4.3 Write short note on VOIP Vulnerabilities and Countermeasures. (Ref. Sec. 4.4.2) (5 Marks)

- The top VoIP vulnerabilities, drawn from the new book "Securing VoIP Networks," by authors Peter Thermos and Ari Takanen, takes a tough look at the weak side of VoIP.
- How are VoIP networks weak and vulnerable to attack and catastrophic failure? ***Securing VoIP Networks***, the new book by Peter Thermos and Ari Takanen, looks at VoIP infrastructure and analyzes its vulnerabilities much as the Open Web Application Security Project did for Web-related vulnerabilities and Mitre did with its ***Common Weakness Enumeration*** dictionary for software. And it's about human failings, too, not just technology problems.
- Here are the top VoIP vulnerabilities explained in **Securing VoIP Networks :**

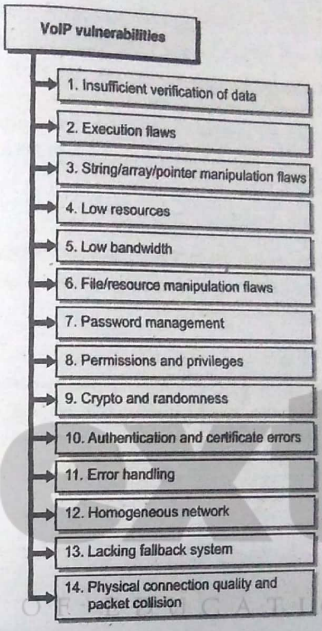

Fig. 4.4.1 : VoIP vulnerabilities

1. Insufficient verification of data:

In VoIP implementations, this can enable man-in the-middle attacks.

2. Execution flaws

Standard databases are typically used as the backbone of VoIP services and registrations. Implementation has to be paranoid in filtering out active content such as SQL queries from user-provided data such as user names, passwords, and Session Initiation Protocol (SIP) URLs. The majority of problems relating to execution flaws result from bad input filtering and insecure programming practices.

3. String/array/pointer manipulation flaws

Malformed packets with unexpected structures and content can exist in any protocol messages, including SIP, H.323, SDP, MGCP, RTP, and SRTP. Most typical malformed messages include buffer-overflow attacks and other boundary-value conditions. The result is that the input given by the attacker is written over other internal memory content, such as registers and pointers, which will let the attacker take full control of the vulnerable process.

4. Low resources

Especially in embedded devices, the resources that VoIP implementations can use can be scarce. Low memory and processing capability could make it easy for an attacker to shut down VoIP services in embedded devices.

5. Low bandwidth

The service has to be built so that it will withstand the load even if every caller makes a call at the same time. When the number of subscribers to a VoIP service is low, this is not a big problem. But when a service is intentionally flooded with thousands of bot clients, or when there is an incident that results in a huge load by valid subscribers, the result might be a shutdown of the whole service.

6. File/resource manipulation flaws

These are typical implementation mistakes, programming errors from using insecure programming constructs that result in security problems. These flaws include insecure access to files.

7. Password management

The only identifier a VoIP consumer has is the telephone number or SIP URL and a possible password for the service. The passwords are stored in both the client and server. If passwords are storied in the server in a format that can be reversed, anyone with access to that server (or proxy or registrar) can collect the username and password pairs.

8. Permissions and privileges

Resources have to be protected both from the operating system and platform perspective and from the network perspective. VoIP services running on the platform have to consider the privileges they run with. A VoIP service does not necessarily require administrative or "root" privilege to run.

9. Crypto and randomness

In VoIP signaling, confidential data needs to be protected from eavesdropping attacks. The most common vulnerability in this category is to fail to encrypt at all, even if the encryption mechanisms are available.

10. Authentication and certificate errors

Users and devices need to be authenticated. Also, other services, such as device management, exist in VoIP devices that need user authentication. Registration hijack in SIP is a flaw in which the registrar system does not authenticate the user or device, but lets attackers spoof registration messages and reregister themselves as the valid user.

11. Error handling

One example of error handling in SIP implementations is how incorrect registration is handled. A register message with an invalid telephone number can result in a "404" error code, whereas a valid telephone number would result in a "401" error. This will let the attacker narrow down the attack to try a brute-force attack on valid accounts only, or to harvest for valid accounts for Spam over Internet Telephony (SPIT).

12. Homogeneous network

An unpredicted vulnerability in many network infrastructures is a wide dependence on a limited number of vendor brands and devices variants. If an entire network depends on one specific brand of phone, proxy or firewall, one automated attack such as a virus or worm can shut down the entire network.

13. Lacking fallback system

When the VoIP network is down, as it eventually will be, there has to be backup systems that the users can fall back to. This requires careful planning for the infrastructure.

14. Physical connection quality and packet collision

If you have packet loss in your data infrastructure, you're probably not ready for VoIP. Network latency and jitter should be minimal. All bottlenecks in the communications will immediately be revealed when VoIP is introduced, even if those weren't readily apparent with traditional data communications.

Syllabus Topic : PBX Security

4.5 Private Branch Exchange (PBX)

Q. 4.5.1 Write a short note on PBX. (Ref. Sec. 4.5) (5 Marks)

- A PBX (Private Branch Exchange) is a telephone system within an enterprise that switches calls between enterprise users on local lines while allowing all users to share a certain number of external phone lines. The main purpose of a PBX is to save the cost of requiring a line for each user to the telephone company's central office.
- The PBX is owned and operated by the enterprise rather than the telephone company (which may be a supplier or service provider, however). Private branch exchanges used analog technology originally. Today, PBXs use digital technology (digital signals are converted to analog for outside calls on the local loop using Plain Old Telephone Service (POTS).
- A PBX includes :
  - Telephone trunk (multiple phone) lines that terminate at the PBX
  - A computer with memory that manages the switching of the calls within the PBX and in and out of it
  - The network of lines within the PBX
  - A console or switchboard for a human operator (optional)
- In some situations, alternatives to a PBX include centre x service (in which a pool of lines are rented at the phone company's central office), key telephone systems, and, for very small enterprises, primary rate Integrated Services Digital Network (ISDN).
- Lucent Technologies, Northern Telecom (NORTEL), Rolm/Siemens, NEC, GTE, Intecom, Fujitsu, Hitachi and Mitel are among the larger manufacturers of PBXs.

Syllabus Topic : TEM : Telecom Expense Management

4.6 Telecom Expense Management (TEM)

Q. 4.6.1 What is TEM? Write its advantages and disadvantages. (Ref. Sec. 4.6) (5 Marks)

- Telecom Expense Management (TEM) is a term used to define an approach to managing all telecommunication service expenses such as voice, data and wireless with a combination of software tools and manual auditing.
- In managing all these services and related processes, its goal is to minimize costs and maximize process efficiency.
- For a small company, it can be as simple as checking over your phone bill every month to make sure you aren't billed for services you don't want.
- For larger companies, it is a more formal program to optimize spending on telecom services. Most of the attention goes to bill auditing and getting refunds for billing errors, but an effective TEM program can do more than that.
- EM provides a structured and professional way to manage the telecom spending of a company, no matter how large or small. This management can be in the form of software used by a manager or an outside telecom expert.

Disadvantages

1) Using multiple carriers for different services that use different invoice formats. This makes it difficult to match and allocate costs effectively;
2) Not having a complete inventory of the company's assets including wireless devices, headsets, hardware, computer networks, etc.
3) Difficulty in being able to apportion telecommunications costs to divisions, teams or departments with any accuracy;
4) Not having the company resources to manually audit each invoice. Between 7-12% of bills are in error. For large companies, this is a substantial amount of money they could be losing every month; and
5) Not understanding costs. You can't control the cost of something when you don't understand how it's billed or what you're getting for your money.

Advantages

- Managing telecom services is complex and requires constant attention. A qualified telecom expert can not only perform systematic audits but can also alert the company to new cost-saving options. Software programs can allow companies to eliminate waste and optimize resources.
- Both software and outside experts can help you to: reduce time through systematized processes; reduce costs through error identification; reduce risks through better reporting options; and increase control and thereby accountability.

- Software will help the Telecom Manager's knowledge and understanding of the products, services and costs for his company's telecom spending. An outside expert can handle disputes with carriers and get price quotes for new services. They can also restructure your agreements and contracts with current providers and find less expensive providers.
- A solid TEM platform will provide a centralized solution for inventory control and procurement, contract compliance, budget and spending tracking, and invoice processing. Proactive systems can alert you to policy breaches and contract compliances.
- Large companies are the prime candidates for Telecom Expense Management. However, small and mid-size companies that need to organize and monitor their telecom spending would benefit as well.
- For most small to mid-size companies telecom spending is the responsibility of an IT person, an office manager, an accountant or a combination of all three.
- For these types of organizations, the benefit of a TEM solution is based on labor saving efficiencies through automation. This benefits both telecom and financial sides of the company by providing a way for them both to monitor, control and report on company telecom.
- Considering the importance of telecommunications in the operation of your daily business, Telecom Expense Management is a critical business strategy. Your company needs to not only track its spending, but also to maximize its telecom resources. TEM lets you make informed decisions rather than educated guesses.

Syllabus Topic : Operating System Security Models : Classic Security Models

4.7 Security Models

Q. 4.7.1 Write short note on security models. (Ref. Sec. 4.7) **(5 Marks)**

4.7.1 Introduction

Security refers to providing a protection system to computer system resources such as CPU, memory, disk, software programs and most importantly information stored in the computer system. If a computer program is run by an unauthorized user, then it may cause severe damage to computer or data stored in it. So a computer system must be protected against unauthorized access, malicious access to system memory, viruses, worms etc. We're going to disçuss following topics in this chapter.

- Authentication.

- One Time Passwords.
- Program Threats.
- System Threats.
- Computer Security Classifications.

Authentication

Authentication refers to identifying each user of the system and associating the executing programs with those users. It is the responsibility of the Operating System to create a protection system which ensures that a user who is running a particular program is authentic. Operating Systems generally identifies/authenticates users using following three ways –

(i) **Username / Password :** User need to enter a registered username and password with Operating system to login into the system.

(ii) **User card/key :** User need to punch card in card slot, or enter key generated by key generator in option provided by operating system to login into the system.

(iii) **User attribute :** Fingerprint/ eye retina pattern/ signature – User need to pass his attribute via designated input device used by operating system to login into the system.

One time passwords

One-time passwords provide additional security along with normal authentication. In One-Time Password system, a unique password is required every time user tries to login into the system. Once a one-time password is used, then it cannot be used again. One-time password is implemented in various ways.

- **Random numbers :** Users are provided cards having numbers printed along with corresponding alphabets. System asks for numbers corresponding to few alphabets randomly chosen.
- **Secret key :** User are provided a hardware device which can create a secret id mapped with user id. System asks for such secret id which is to be generated every time prior to login.
- **Network password :** Some commercial applications send one-time passwords to user on registered mobile/ email which is required to be entered prior to login.

Program threats

Operating system's processes and kernel do the designated task as instructed. If a user program made these process do malicious tasks, then it is known as **Program Threats**. One of the common example of program threat is a program installed in a computer which can store

and send user credentials via network to some hacker. Following is the list of some well-known program threats.

- **Trojan Horse :** Such program traps user login credentials and stores them to send to malicious user who can later on login to computer and can access system resources.
- **Trap Door :** If a program which is designed to work as required, have a security hole in its code and perform illegal action without knowledge of user then it is called to have a trap door.
- **Logic Bomb :** Logic bomb is a situation when a program misbehaves only when certain conditions met otherwise it works as a genuine program. It is harder to detect.
- **Virus :** Virus as name suggest can replicate themselves on computer system. They are highly dangerous and can modify/delete user files, crash systems. A virus is generally a small code embedded in a program. As user accesses the program, the virus starts getting embedded in other files/ programs and can make system unusable for user

☞ **System threats**

System threats refers to misuse of system services and network connections to put user in trouble. System threats can be used to launch program threats on a complete network called as program attack. System threats creates such an environment that operating system resources/ user files are misused. Following is the list of some well-known system threats.

- **Worm :** Worm is a process which can choked down a system performance by using system resources to extreme levels. A Worm process generates its multiple copies where each copy uses system resources, prevents all other processes to get required resources. Worms processes can even shut down an entire network.
- **Port Scanning :** Port scanning is a mechanism or means by which a hacker can detects system vulnerabilities to make an attack on the system.
- **Denial of Service :** Denial of service attacks normally prevents user to make legitimate use of the system. For example, a user may not be able to use internet if denial of service attacks browser's content settings.

4.7.2 Computer Security Classifications

Q. 4.7.2 Write short note on Computer Security Classifications. (Ref. Sec. 4.7.2) (5 Marks)

As per the U.S. Department of Defense Trusted Computer System's Evaluation Criteria there are four security classifications in computer systems: A, B, C, and D. This is widely used

specifications to determine and model the security of systems and of security solutions. Following is the brief description of each classification.

Table 4.7.1

S.N.	Classification Type and Description
1	**Type A** Highest Level. Uses formal design specifications and verification techniques. Grants a high degree of assurance of process security.
2	**Type B** Provides mandatory protection system. Have all the properties of a class C2 system. Attaches a sensitivity label to each object. It is of three types. – **B1 :** Maintains the security label of each object in the system. Label is used for making decisions to access control. – **B2 :** Extends the sensitivity labels to each system resource, such as storage objects, supports covert channels and auditing of events. – **B3 :** Allows creating lists or user groups for access-control to grant access or revoke access to a given named object.
3	**Type C** Provides protection and user accountability using audit capabilities. It is of two types. – **C1 :** Incorporates controls so that users can protect their private information and keep other users from accidentally reading / deleting their data. UNIX versions are mostly Cl class. – **C2 :** Adds an individual-level access control to the capabilities of a Cl level system.
4	**Type D** Lowest level. Minimum protection. MS-DOS, Window 3.1 fall in this category.

- The essence of information security is to protect information. It is just that simple. So whenever possible do not make it more complicated than needed. Complexity for cyber

security and privacy arise when information needs to be shared or must be made accessible by some digital device.

- The world where information was only available in physical archives is long gone. The focus from physical information security is shifted to cyber information security. But be aware: Crucial principles of centuries of physical information protection are still valuable today.
- Especially principles related to the intangible soft issues when information is shared. Ever wondered how some organizations managed to keep their valuable information secret for many decades?
- Information protection is needed against unauthorized access, use, disclosure, modification or destruction. That means several security measures are needed to protect information from unauthorized viewers.
- Measures can be implemented by procedural, physical or with complex IT tools. But before classifying and creating or finding good measures it is essential that the problem field is made clear.
- Creating effective solutions for information security problems can be done by creating a model of the problem situation. Within a model all elements that relate with the problem situation are brought together to study effective solutions.
- Without going into detail on system science or problem solving theory: in general systems consist of sub-systems, objects, functions or processes, and activities or tasks.
- The key in creating a good model to solve a specific information security problem is to model the problem, not the complete system with all elements. This because modelling the world completely is ineffective, time consuming and it does not give a direct answer to solve a problem situation. It is far better to start with a small model of a problem and create extensions on this model if needed.
- The field of modelling problem situations to solve information security problems is not new. Many models in literature exist. Reusing a good model can save you time and safeguards you from making mistakes.
- A prerequisite is that you start with a good model that can be trusted and is intensively reviewed by large numbers of subject matter experts.
- There are many good security models that can assist in creating a solution architecture to solve a specific security problem for an organization. Mind that a model can be expressed in many different forms.

E.g. :

- One or more images;
- Text;
- Software model

Within the field of modelling a distinction can be made between 'hard' and 'soft' models. Hard models are often mathematical (risk) models whereas soft models are more quality based models. Since using hard models often gives a false sense of reliability and requires full insight of all assumptions made it is more productive to reuse soft security and privacy models. When creating solution architecture, you need:

- A threat model (what are the threats your solution gives protection against).
- Insight in commonly used attack vectors. This means you need to have some view on the attack vectors used in the use case?

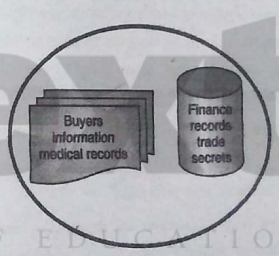

Fig. 4.7.1

- Creating a good security or privacy design or architecture means you never ever start with selecting tools for solving your problem! Selecting tools should be the last phase of your security or privacy design phase.
- You select tools when it is clear that the tool will support in solving your security or privacy problem. Tools alone are never enough to solve security or privacy problems. You need to fit in tools within your security and privacy processes.
- Several problems exist with many IT security tools that will hit you when you start too soon with the solutions instead of a thorough problem diagnosis and solution design. Wrongly selected security and privacy tools give the following issues :
  - High costs.
  - Complex challenges to implement and manage.

- Daily administration of a chosen tool set requires significant IT effort while it remains unclear if the tools are effective in reducing security risk.
- Overlap in functionality of security application landscape. More is not always better.

To be able to justify the application of security tools for your problem a context specific security architecture should give input to the following questions :

- What is protected with what ?
- What are the main threats we need protection against ?
- What is not protected by information security policies or tools ?
- What is in scope or out of scope for your security architecture ?
- E.g. business continuity management, safety management, financial risk management, daily IT operations, physical (building) security etc. In the end everything has a relation with information security, but you cannot cover all business aspects using an information security architecture document. The key is to focus and keep the scope clear or else complexity will become overwhelming.
- What architecture or design decisions have been made and must be validated explicitly ?
- What is the model of your protection?
- It is far more easy to evaluate and improve a model, than adding new or improved security products continuously. Make sure that within operational security management processes learning and improving are key periodic targets.
- Does the security model cover all crucial security and privacy principles and requirements?
- Are the residual risks when this solution acceptable for the key stakeholders ?

- IT security in general is seen as a complex problem field, due to the many technical and nontechnical aspects involved. Since 100% information security is impossible, being able to qualify risks is crucial in getting an accepted level of security protection. Good modelling helps you to qualify security and privacy risks.

- In general, it is far more easy to reuse proven concepts and models when creating your own security model. This way you build on the work of others and using a good model reference will reduce the risk of making crucial mistakes.
- This section covers some commonly used models and elements that can be reused when creating a solution for a specific information security problem.
- Elements that are presented are attack vectors, some examples of security personas and some great security models that can assist you when creating your security design.

Syllabus Topic : Operating System Models

4.7.3 Operating System Models

Q. 4.7.3 Explain Operating System Model. (Ref. Sec. 4.7.3) **(2 Marks)**

- Operating System security (OS security) is the process of ensuring OS integrity, confidentiality and availability. OS security refers to specified steps or measures used to protect the OS from threats, viruses, worms, malware or remote hacker intrusions. OS security encompasses all preventive-control techniques, which safeguard any computer assets capable of being stolen, edited or deleted if OS security is compromised.
- OS security encompasses many different techniques and methods which ensure safety from threats and attacks.
- OS security allows different applications and programs to perform required tasks and stop unauthorized interference. OS security may be approached in many ways, including adherence to the following :
- Performing regular OS patch updates.
- Installing updated antivirus engines and software.
- Scrutinizing all incoming and outgoing network traffic through a *firewall*.
- Creating secure accounts with required privileges only (i.e., user management).

Syllabus Topic : Reference Monitor

4.7.4 Reference Monitor

Q. 4.7.4 Explain Reference Monitor. (Ref. Sec. 4.7.4) **(2 Marks)**

- In operating systems architecture, a reference monitor is a secure, always-used and fully-testable module that controls all software access to data objects or devices. The reference monitor verifies the nature of the request against a table of allowable access types for each process on the system. For example, Windows 3.x and 9x operating systems were not built with a reference monitor, but it was added to Windows starting with Windows NT.
- A component of the Microsoft Windows NT executive running in kernel mode that acts like a security watchdog, enforcing security when applications try to access system resources.
- The Security Reference Monitor decides whether a given process should be granted access rights to an object. It does this by comparing the access token attached to the process to the Discretionary Access Control List (DACL) attached to the object that the process is trying to access.
- It compares the Security identifiers (SIDs) in the DACL entry by entry to the SIDs in the access token to see what level of access the process should be granted. If any of the DACL SIDs denies the request access, the process is denied access to the object. The Security Reference Monitor also ensures that auditing takes place if auditing is configured in the local security policy.

Syllabus Topic : Trustworthy Computing

4.7.5 Trustworthy Computing

Q. 4.7.5 What is trustworthy computing? (Ref. Sec. 4.7.5) (5 Marks)

- Trust worthy computing is a broad term that refers to technologies and proposals for resolving computer security problems through hardware enhancements and associated software modifications.
- Several major hardware manufacturers and software vendors, collectively known as the Trustworthy Computing Group (TCG), are cooperating in this venture and have come up with specific plans.
- The TCG develops and promotes specifications for the protection of computer resources from threats posed by malicious entities without infringing on the rights of end users.

- Microsoft defines trust worthy computing by breaking it down into four technologies, all of which require the use of new or improved hardware at the Personal Computer (PC) level :

Memory curtaining :

Prevents programs from inappropriately reading from or writing to each other's memory.

Secure input/output (I/O) :

Addresses threats from spyware such as keyloggers and programs that capture the contents of a display.

Sealed storage :

- Allows computers to securely store encryption keys and other critical data.

Remote attestation :

Detects unauthorized changes to software by generating encrypted certificates for all applications on a PC.

- In order to be effective, these measures must be supported by advances and refinements in the software and Operating Systems (OSs) that PCs use.
- Within the larger realm of trust worthy computing, the Trustworthy Computing Base(TCB) encompasses everything in a computing system that provides a secure environment. This includes the OS and its standard security mechanisms, computer hardware, physical locations, network resources and prescribed procedures.
- The term trust worthy PC refers to the industry ideal of a PC with built-in security mechanisms that place minimal reliance on the end user to keep the machine and its peripheral devices secure.
- The intent is that, once effective mechanisms are built into hardware, computer security will be less dependent on the vigilance of individual users and network administrators than it has historically been.
- Concerns have arisen, however, about possible loss of user privacy and autonomy as a result of such changes.

4.8 Common Attack Vectors

Q. 4.8.1 Write short note on Common attack vectors. (Ref. Sec. 4.8) (5 Marks)

- Good security is goal oriented. Good security architecture is tailored to your situation. When defining a product or new (IT) service one of the key activities is to define your specific security requirements. Defining requirements is known to be hard, time consuming and complex. Especially when you have iterative development cycles and you do not have a clear defined view of your final product or service that is to be created.
- Defining attack vectors within your security requirements documentation is proven to be helpful from the start. Attack vectors will give more focus on expected threats so you can start developing security measures that really matter in your situation from the start.
- Attack vectors are routes or methods used to get into information systems. Attacks are the techniques that attackers use to exploit the vulnerabilities in applications. Many attack vectors take advantage of the human element in the system or one of the maintenance activities defined for the system, because that's often defined as the weakest link.
- Within the IT cyber security world many terms and definitions are used. Attack vectors usually require detailed knowledge to judge whether the vector is relevant in a specific situation.
- Some attack vectors apply to critical infrastructure components, like NTP or DNS. E.g. in a rogue master attack, an attacker causes other nodes in the network to believe it is a legitimate master. Contrary to spoofing attacks in the Rogue Master attack the attacker does not fake its identity, but rather manipulates the master election process using malicious control packets.
- The good news is: The number of possible attack vectors is limited. The bad news is: The ways an attack vector can be exploited is endless. Unless decent security measures are taken to minimize attacks using this specific attack vector. Good designed security solutions are not that complicated and complex after all.
- **Common attack vectors are :**
  - Analysis of vulnerabilities in compiled software without source code.
  - Anti-forensic techniques.
  - Automated probes and scans.
  - Automated widespread attacks.
  - Client validation in AJAX routines.
  - Cross-site scripting in AJAX.
  - Cryptographic Performance Attacks.
  - Cyber-threats & bullying (not illegal in all jurisdictions).

  - DoS Attacks.
  - Email propagation of malicious code.
  - Executable code attacks (against browsers).
  - Exploiting Vulnerabilities.
  - GUI intrusion tools.
  - Industrial espionage.
  - Internet social engineering attacks.
  - Malicious AJAX code execution.
  - Network sniffers.
  - Packet Manipulation.
  - Packet spoofing.
  - Parameter manipulation with SOAP.
  - Replay Attack.
  - RIA thick client binary vector.
  - Rogue Master Attack.
  - RSS Atom Injection.
  - Session-hijacking.
  - Sophisticated botnet command and control attacks.
  - Spoofing.
  - Stealth and other advanced scanning techniques.
  - Targeting of specific users.
  - Web service routing issues.
  - Wide-scale trojan distribution.
  - Wide-scale use of worms.
  - Widespread attacks on DNS infrastructure.
  - Widespread attacks using NNTP to distribute attack.
  - Widespread, distributed denial-of-service attacks.
  - Windows-based remote access trojans (Back Orifice).
  - WSDL scanning and enumeration.
  - XML Poisoning.

- XPATH injection in SOAP message.

– It is recommended that you specify in your solution architecture the attack vectors that apply to your use case. Remember to put the explanation of the attack vectors used in an appendix, since not all your stakeholders will know what e.g. 'Spoofing' is.

4.9 Hosting, Hardware, Firmware and Other Invisible Threats

Q. 4.9.1 Write short note on Hosting, Hardware, Firmware and Other Invisible Threats. (Ref. Sec. 4.9) **(5 Marks)**

– Computer security has become much harder to manage in recent years. This is due to the fact that attackers continuously come up with new and more effective ways to attack our systems. But also the emerging trend of Cloud Computing created an extra level of complexity within the field of cyber security and privacy protection.

– A commonly wide spread fad is that Cloud Hosting is more secure than on premise. The truth is that it is different. Security principles and all attack vectors still apply. The main factors that make Cloud hosting more complex to manage are :

- Less control.
- Technical insight in exact physical and IT security measures are often unknown.
- Influence and control on continuous operational changes on the cloud hosting facilities are not transparent for cloud consumers.
- Trust plays a great role. You must have trust in audit and security reports created by a third party. The advice is to obtain always a right to perform a security audit yourself, but at large cloud hosting providers this is often not allowed.

– Whether you use Cloud hosting of host your computer services still on your own data centre all hardware threads still apply.

– Since true open source hardware is still seldom seen, currently your valuable information is vulnerable due to the following more hardware related attack vectors :

- BIOS attacks. BIOS is always written to a non-volatile storage device such as an EEPROM.
- Firmware attacks.
- Physical device tempering. Mostly done by rewiring CPU's, CPU boards. Famous are of course the attacks on Crypto Devices (HSM's) but since hardware tempering on normal hardware is so easy you seldom hear how easy hacking on 'standard' computer hardware devices is.

- Physical data centres. Your data is not (never) secure in a cloud you do not control or manage.

– An attack vector that many people forget to consider is the boot process itself which is almost completely controlled by the BIOS.

– When you are still in control of your own computer hardware, consider to overcome the malicious attacks on BIOS by one the following methods :

- Digital Authentication Method.
- Rollback Prevention Method.
- Physical Authentication Method.

– Threads related to hardware are often invisible. This does not mean they don't exist. Since computer hardware is seldom open, many threads are still not widely known. In order to protect your core information you should always take measures to be able to reduce the likelihood of getting targeted by attack vectors that are hardware related. Many examples exist of poor designed CPU's, firmware, network devices, storage devices etc. with offers great opportunities to attackers.

4.9.1 Security Personas

– Humans are the most important threat to security and privacy.

– One of the tools of IT architects and UX designers is to work with so called 'Personas'. Personas are fictional characters created to represent the different user types that might use a system, website, product or service.

– Using personas is common practice when dealing with UX design. But when developing a security architecture for a new system, service or website security personas are also valuable to use. Security Personas force you to think different about the goals and behaviour of attackers that are going to hit your system.

– Security Personas identify the user motivations, expectations and goals responsible for driving bad behaviour. Of course not all personas will behave bad on purpose. Sometimes mistakes on the use of the system or social engineering will affect the way a persona can compromise your system.

4.9.2 Benefits of Personas

Q. 4.9.2 What are the benefits of Personas? (Ref. Sec. 4.9.2) **(5 Marks)**

Personas help to focus and help to make design decisions concerning IT components by adding a layer of real-world consideration to the conversation. They also offer a quick and

inexpensive way to test and prioritize those features throughout the development process. In addition, they can help :

- Stakeholders and management to discuss architecture building blocks to protect your system.
- Information architects develop informed secure wire-frames knowing possible interface behaviour.
- System security engineers/developers to decide which approaches to take based on user behaviours.
- Testing

For security personas it is good to outline :

- Demographics such as age, education, ethnicity, and family status.
- The goals and tasks they are trying to complete using the system (or website),
- Their physical, social, and technological environment.
- Responsibilities: As implemented in future Identity and access management system, but also the formal organization responsibilities belong to the role within the organization.

Defining security personas is not hard. Some examples of security personas :

- Employee
- Visitor (in person)
- Internet visitor (web)
- Administrator
- Manager
- Director/CEO
- Angry customer
- Competitor/rival
- Neighbours

Use security personas in your security architecture so the proposed security measures can be designed more in depth and evaluated since the security personas are part of your security model. The list given in this section can be used as starting point to expand the personas for your context more in depth.

4.10 Threat Models

- This section is not about teaching you how to model you specific security or privacy solutions. By now you know that your model should be built out of attack vectors, security personas and security and privacy principles and requirements.
- First we present valuable models that can be reused when created a security or privacy solution architecture.
- Security threat modelling, or threat modelling, is a process of assessing and documenting a system's security risks. Security threat modelling enables you to understand a system's threat profile by examining it through the eyes of your potential attackers.
- Your security threat modelling efforts also enable your team to justify security features within a system, or security practices for using the system, to protect your corporate assets.
- Many ways exist to build a threat model but in essence a threat model is a conceptual model that :
  - Helps to understand a situation and
  - Is helpful in reducing security or privacy concerns. So helpful in solving your security problem.
- A security or privacy conceptual threat model is usually built of relevant elements and their relations that matter in a security problem situation.
- In general, a conceptual model is constructed based on a specific problem situation you want to solve. In our case the aim is to outline important concepts regarding security and privacy.
- So our collection of conceptual models is aimed at generic reuse. Since the real-world problems of security and privacy are outlined in a large number of publications, within this section we only present conceptual models that are based on the following selection criteria :
  - Generic use;
  - Non-commercial;
  - Open.
- With open we mean that the institute or company created the model has an open process that allows everyone to improve the model. Of course open is not always really open without borders and thresholds.

- Even the open group is not really open for public participation, since large memberships fees form a threshold. The OWASP foundation is however one of the best examples on how open should be.
- That is open license on content (common creative) and no impediments and no requirements for participants who want to join the working groups.
- For security and privacy many models exist. Most models are aimed for evaluating risks for auditors and other stakeholders. In the sections below a collection of (almost open) security and privacy models.

4.10.1 Privacy Management Reference Model

Q. 4.10.1 Explain Privacy Management Reference Model with suitable diagram. (5 Marks)
(Ref. Sec. 4.10.1)

The Privacy Management Reference Model and Methodology (PMRM) of the OASIS group provides a model and a methodology for :

- Understanding and analysing privacy policies and their privacy management requirements in defined use cases; and
- Selecting the technical services which must be implemented to support privacy controls.
- The model is particularly relevant to evaluate use cases in which Personal Information (PI) flows across regulatory, policy, jurisdictional and system boundaries.

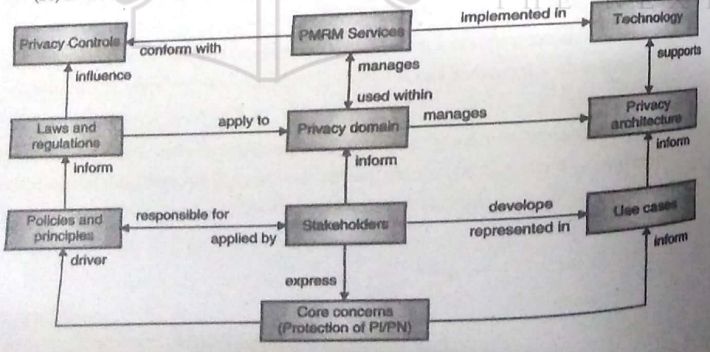

Fig. 4.10.1

- More in-depth information regarding this model can be found on the OASIS site (see references).

4.10.2 NIST Security Framework

- Whenever you feel the need to draw a process regarding security or risk processes: resist the temptation! The US based NIST organization is a well-known governmental organization that offers great publications on all thinkable subjects regarding security.
- One of the simplest, yet most frequently model is displayed here below.

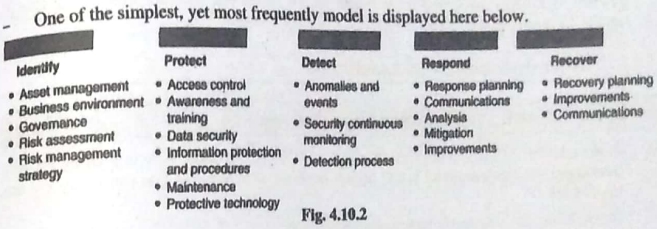

Fig. 4.10.2

- On the NIST site (see references) you can find in-depth information regarding all sub functions of this security framework.
- The experience is, is that it is far better to check what in your use case needs special attention. If you ever feel the need to create your own security framework, think again. In essence all come down to the high level framework described by the NIST organization. Using a broad used security framework has a number of advantages :
  - Easier communication with stakeholders;
  - Easier knowledge and experience transfer between security experts of different organization;
  - Saves time, time you can use to solve the real context specific issues regarding practice use and implementation of the security functions.

4.10.3 Jericho Security Model

The Jericho(tm) Security architecture model is built upon principles. The advantages of using the Jericho model for security are :

- A security architecture model built upon the Jericho conceptual model is built around maintaining flexibility and protects the most important security objects for the stakeholders.
- Integration : Easier to build secure processes with other companies and trusted partners.
- Simplifies use of public networks and cloud solutions.
- Aimed for use of open principles and open solution building blocks.

- Unfortunate the Jericho framework is not a real open security framework. It is copyrighted by the open group (see references chapter for more information on this model). There are trademarks involved and all publications are copyrighted.
- However due to the work of many we can make use of the developed knowledge within the Jericho working group. The Jericho Forum®, a forum of The Open Group, was formed in January 2004 and is no longer active. However, the approach of this forum towards security is still alive.

4.11 Security Architecture Landscape

Q. 4.11.1 Explain OSA with suitable diagram. (Ref. Sec. 4.11) (5 Marks)

- Thanks to the Open Security Architecture (OSA) group there is a real open security landscape. All OSA material is CC by SA licensed, which means you can freely use and improve it.

Below is the OSA Security architecture landscape :

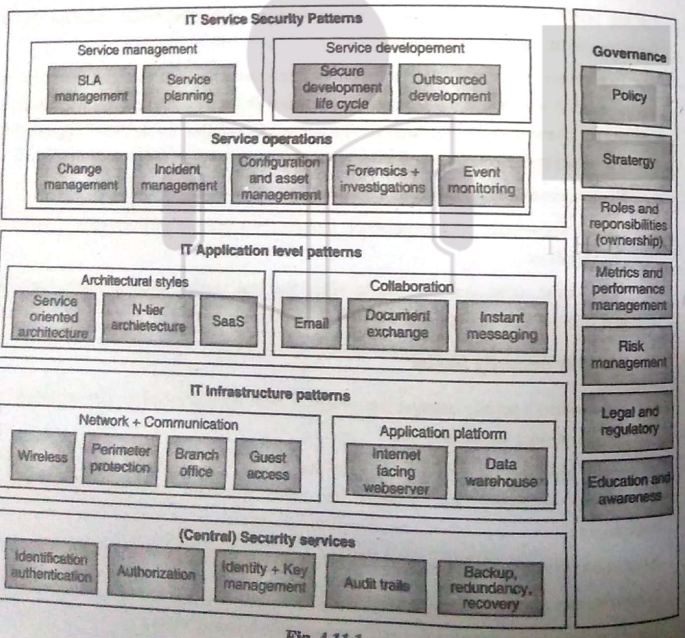

Fig. 4.11.1

- The OSA Security architecture is based on patterns. Which mean for every pattern defined the aim of the community was/is to develop a standardized solution description. Unfortunate the OSA community is not very active anymore, so all IT security patterns around cloud are not yet incorporated.
- For a number of reasons we have chosen not to use patterns in this security and privacy reference architecture. However in some cases using patterns can give an advantage. (See the Introduction, section 'What about security patterns?' for more information).

4.12 Software Assurance Maturity Model (SAMM)

Q. 4.12.1 Write short note on SAMM. (Ref. Sec. 4.12) (5 Marks)

- The Software Assurance Maturity Model (SAMM) is an open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization.
- SAMM is useful resource if you are working on a process architecture that is needed to control all kind of aspects of software security.
- Our advice is to take the processes as defined in SAMM as point of departure within your security process design documentation. Formulating processes yourself in not productive, so use this valuable source of information instead of reinventing the wheel.
- To get the baseline situation of your security process architecture fast in scope, you can use a SAMM self-assessment test. Using a self-assessment test you can get a very quick overview on the status of the IT security processes within your organization. SAMM is an OWASP project.

SAMM will aid in

- Evaluating an organization's existing software security practices,
- Building a balanced software security assurance program in well-defined iterations.
- Demonstrating concrete improvements to a security assurance program.
- Defining and measuring security-related activities throughout an organization.

As an open project, SAMM content shall always remain vendor-neutral and freely available for all to use.

Source : OWASP

- Reuse of the SAMM process and usage should be encouraged. This OWASP project is like all OWASP projects a real open project. All content is available under a Creative

Commons License (by-sa). If you want to improve this SAMM framework, OWASP is a real open foundation where everyone can participate without borders. Also all communication and collaboration is truly open.

- The SAMM model was first aimed at evaluating the status of software security within an organization. However due to the use in practice the framework can also be used to improve many other aspects surrounding security and privacy.

4.13 Security within the SDLC process

Q.4.13.1 Explain SDLC with suitable diagram. (Ref. Sec. 4.13) (5 Marks)

- The view below (source OWASP) is a model of how security fits into the SDLC (Software Development and Lifecycle) process. Within almost every solution architecture you should take the SDLC into account to position where your solution fits and how maintenance is positioned within the SDLC phases.

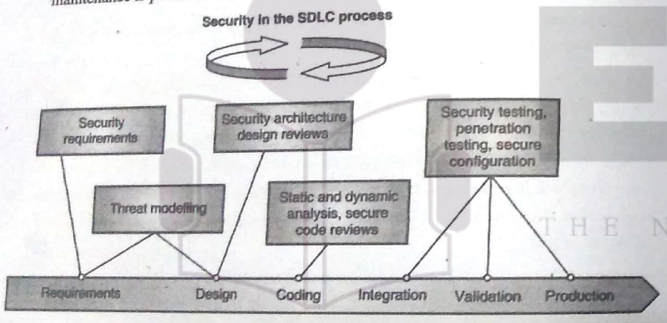

Fig. 4.13.1

- Security and privacy should be embedded in the SDLC process. The OWASP conceptual model of the (simplified) SDLC chain shows on high level where security activities hit the SDLC process.

4.14 IoT Threat Model

Q.4.14.1 Explain IoT threat model with suitable diagram. (Ref. Sec. 4.14) (5 Marks)

- We should be happy : The IoT (Internet of Things) is not everywhere present yet. When IoT is migrated from fiction to reality, security and privacy will be under enormous risks.
- Internet-of-Things is a result of a technical revolution, which reflects with future computing and communications including existing and evolving internet. Over the time Internet technologies have evolved, and become Internet of Things. With the advent of this paradigm the dream to convergence everything, and everyone under a single umbrella has come true.
- Machine-to-Machine (M2M), Radio Frequency Identification (RFID), context-aware computing, wearables, ubiquitous computing, and web-of-things all are considered to be seamlessly integrated into a global information network, which has the self configuring capabilities based on standard and inter-operable communication protocols.
- Below a generic threat model for the IoT world :

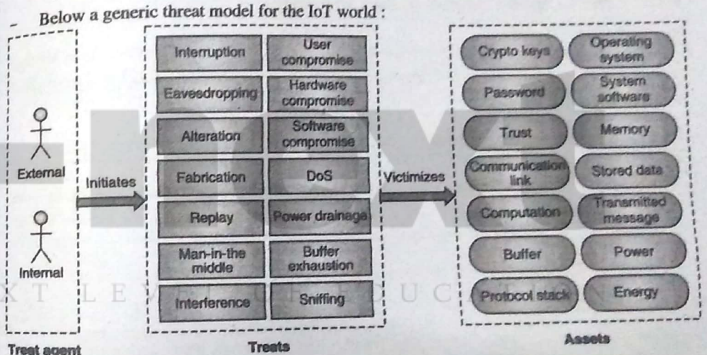

Fig. 4.14.1

- Note the view is not complete. Missing these views are : IDS, pentest tools, correlation tools etc (or under system security).

This IoT thread model and views are good for addressing the following areas in more detail in your security solution :

- Confidentiality.
- Integrity.
- Availability.
- User Management.

- Network Security.
- Key Management.
- Security Management.
- Governance.
- Risk.
- Regulation.
- Audit.
- Access Control.
- Standards for Interoperability.

4.15 NIST Cloud Computing Security Model

Sooner or later you will be creating a solution or privacy architecture where cloud hosting plays a significant part. The NIST cloud computing security reference model is a very good model to use as reference.

4.16 Mobile Threat Model

- Since mobile is everywhere, you should always take mobile threats serious in your solution architecture. Even if you think you have a special gateway for mobile traffic, most devices are always vulnerable for mobile threads.
- The model presented here below can help in identifying the threads.

4.17 DDoS Model

Q.4.17.1 Explain DDoS. (Ref. Sec. 4.17) **(5 Marks)**

- DDoS attacks are hard to prevent. However, every security or privacy architecture should take DDoS attacks into account. This to design solution that is more resistant against the easy DDoS attacks.

Problems due to DDoS Attacks

- DDoS attack is an attempt to make a systems inaccessible to its legitimate users.
- The bandwidth of the Internet and a LAN may be consumed unwontedly by DDoS, by which not only the intended computer, but also the entire network suffers.
- Slow network performance (opening files or accessing web sites) due to DDoS attacks.

- Unavailability and inability to access a particular web site due to DDoS attacks.
- The model below gives a DDoS attack taxonomy. This can be useful if you are designing solutions to be more resilient against DDoS attacks.

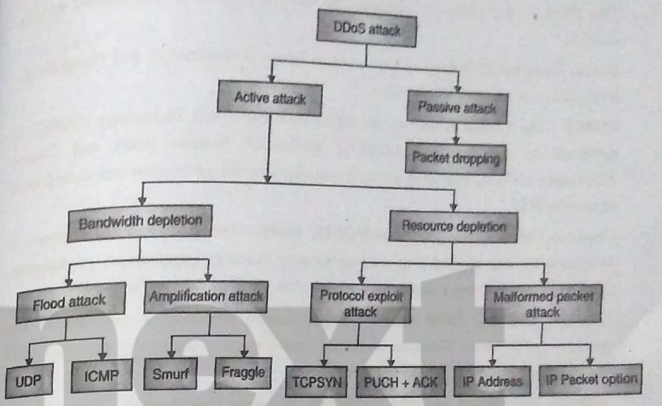

Fig. 4.17.1

Syllabus Topic : International Standards for Operating System Security

4.18 International Standards for Operating System Security

Q. 4.18.1 Write short note on International Standards for Operating System Security. (Ref. Sec. 4.18) **(5 Marks)**

IT Governance Standards and Best Practices

- **ISO/IEC 27000 family of Information Security Management Systems :** This document provides an overview of ISO/IEC 27000 family of Information Security Management Systems which consists of inter-related standards and guidelines, already published or under development, and contains a number of significant structural components.

- **ISO 27001 :** This document provides the ISO standards of the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.
- **ISO 27002 :** This document introduces the code of practice for information security controls.
- **British Standard 7799 Part 3 :** This set of guidelines is published by BSI Group for the information security risk management.
- **COBIT :** The Control Objectives for Information and related Technology (COBIT) is published by the Standards Board of Information Systems Audit and Control Association (ISACA) providing a control framework for the governance and management of enterprise IT.
- **Common Criteria (also known as ISO/IEC 15408) :** This set of evaluation criteria is developed by and aligned with national security standards organisations of Australia, Canada, France, Germany, Japan, Netherlands, New Zealand, Spain, UK and US.
- **ITIL (or ISO/IEC 20000 series) :** This document introduces a collection of best practices in IT Service Management (ITSM), and focuses on the service processes of IT and considers the central role of the user.
- **National Information Security Technology Standard Specification :** This webpage introduces a collection of national information security standards formulated by the National Information Security Standards Technical Committee. These standards include information security management, information security evaluation, authentication and authorisation, etc.
- **SANS Security Policy Resource :** These resources are published by SANS Institute for the rapid development and implementation of information security policies.

4.19 Exam Pack (Review Questions)

☞ **Syllabus Topic : Intrusion Detection System : Concepts, Detection Models, IDS Features**

Q. 1 Write short note on IDS. (Refer Section 4.1) **(5 Marks)**

☞ **Syllabus Topic : IDS Types**

Q. 2 What are the different types of IDS? (Refer Section 4.1.2) **(5 Marks)**

☞ **Syllabus Topic : Intrusion Prevention Systems**

Q. 3 Write short note on IPS. (Refer Section 4.2.1) **(5 Marks)**

Q. 4 What are the different detection methods? (Refer Section 4.2.2) **(5 Marks)**

☞ **Syllabus Topic : IDS Deployment Consideration**

Q. 5 Write a short note on IDS deployment consideration. (Refer Section 4.2.3) **(5 Marks)**

Q. 6 Differentiate between IPS and IDS. (Refer Section 4.2.4) **(5 Marks)**

☞ **Syllabus Topic : Security Information and Event Management (SIEM)**

Q. 7 Write short note on Security Information and Event Management. (Refer Section 4.3) **(5 Marks)**

☞ **Syllabus Topic : Voice over IP (VoIP) : Background**

Q. 8 What is VoIP? Explain VoIP protocols. (Refer Section 4.4) **(5 Marks)**

☞ **Syllabus Topic : VoIP Components**

Q. 9 What are the components of VoIP? (Refer Section 4.4.1) **(5 Marks)**

☞ **Syllabus Topic : VOIP Vulnerabilities and Countermeasures**

Q. 10 Write short note on VOIP Vulnerabilities and Countermeasures. (Refer Section 4.4.2) **(5 Marks)**

☞ **Syllabus Topic : PBX Security**

Q. 11 Write a short note on PBX. (Refer Section 4.5) **(5 Marks)**

☞ **Syllabus Topic : Telecom Expense Management**

Q. 12 What is TEM? Write its advantages and disadvantages. (Refer Section 4.6) **(5 Marks)**

☞ **Syllabus Topic : Operating System Security Models : Classic Security Models**

Q. 13 Write short note on security models. (Refer Section 4.7) **(5 Marks)**

Q. 14 Write short note on Computer Security Classifications. (Refer Section 4.7.2) **(5 Marks)**

☞ **Syllabus Topic : Operating System Models**

Q. 15 Explain Operating System Model. (Refer Section 4.7.3) **(2 Marks)**

☞ **Syllabus Topic : Reference Monitor**

Q. 16 Explain Reference Monitor. (Refer Section 4.7.4) **(2 Marks)**

☞ **Syllabus Topic : Trustworthy Computing**

Q. 17 What is trustworthy computing? (Refer Section 4.7.5) **(5 Marks)**

Q. 18 Write short note on Common attack vectors. (Refer Section 4.8) **(5 Marks)**

Q. 19 Write short note on Hosting, Hardware, Firmware and Other Invisible Threats. (Refer Section 4.9) **(5 Marks)**

Q. 20 What are the benefits of Personas? (Refer Section 4.9.2) **(5 Marks)**

Q. 21 Explain Privacy Management Reference Model with suitable diagram. (Refer Section 4.10.1) **(5 Marks)**

Q. 22 Explain OSA with suitable diagram. (Refer Section 4.11) **(5 Marks)**

Q. 23 Write short note on SAMM. (Refer Section 4.12) **(5 Marks)**

Q. 24 Explain SDLC with suitable diagram. (Refer Section 4.13) **(5 Marks)**

Q. 25 Explain IoT threat model with suitable diagram. (Refer Section 4.14) **(5 Marks)**

Q. 26 Explain DDOS. (Refer Section 4.17) **(5 Marks)**

Syllabus Topic : International Standards for Operating System Security

Q. 27 Write short note on International Standards for Operating System Security. (Refer Section 4.18) **(5 Marks)**

Chapter Ends...

❑❑❑

CHAPTER 5 — Unit V

Virtual Machines and Cloud Computing

Syllabus Topic : Virtual Machines

5.1 Virtual Machines

Q. 5.1.1 Explain virtual machines and give its advantages and drawbacks. (Ref. Sec. 5.1) **(5 Marks)**

- A virtual machine is a computer file, typically called an image, which behaves like an actual computer. In other words, creating a computer within a computer.
- It runs in a window, much like any other programme, giving the end user the same experience on a virtual machine as they would have on the host operating system itself.
- The virtual machine is sandboxed from the rest of the system, meaning that the software inside a virtual machine cannot escape or tamper with the computer itself. This produces an ideal environment for testing other operating systems including beta releases, accessing virus-infected data, creating operating system backups and running software or applications on operating systems for which they were not originally intended.
- Multiple virtual machines can run simultaneously on the same physical computer. For servers, the multiple operating systems run side-by-side with a piece of software called a hypervisor to manage them, while desktop computers typically employ one operating system to run the other operating systems within its programme windows. Each virtual machine provides its own virtual hardware, including CPUs, memory, hard drives, network interfaces and other devices.
- The virtual hardware is then mapped to the real hardware on the physical machine which saves costs by reducing the need for physical hardware systems along with the associated maintenance costs that go with it, plus reduces power and cooling demand.