Chapter 6 ................................................................................................................................. 3

Network Security Controls ........................................................................................................... 3

6.1 Introduction ............................................................................................................................ 3

6.2 Network Characteristics ....................................................................................................... 3

6.3 Threats and Vulnerabilities .................................................................................................. 4

6.3.1 Information Gathering ....................................................................................................... 5

6.3.2 Exploiting communication subsystem vulnerabilities ...................................................... 6

6.3.3 Protocol Flaws .................................................................................................................. 7

6.3.4 Impersonation .................................................................................................................... 7

6.3.5 Message Confidentiality Threats ....................................................................................... 9

6.3.6 Message Integrity Threats .................................................................................................. 9

6.3.7 Web Site Defacement ....................................................................................................... 10

6.3.8 Denial of Service ............................................................................................................... 10

6.3.9 Distributed Denial of Service ............................................................................................ 11

6.3.10 Threats from Cookies, Scripts and Active or Mobile Code ............................................ 11

6.3.11 Malicious Code ............................................................................................................... 11

6.3.12 Virus / Malicious Code protection mechanisms: ............................................................ 13

6.4 Current Trends in attacks .................................................................................................... 14

6.4.1 Exploiting application vulnerabilities ................................................................................. 14

6.4.2 Advanced persistent threat (APT) ...................................................................................... 15

6.5 Network Security Controls .................................................................................................. 15

6.5.1 Architecture ...................................................................................................................... 16

6.5.2 Cryptography/Encryption ................................................................................................ 17

6.5.3 Content Integrity ............................................................................................................... 21

6.5.4 Strong Authentication ....................................................................................................... 23

6.5.5 Remote Access Security ................................................................................................... 23

6.5.6 Firewalls ............................................................................................................................ 24

6.5.7 Intrusion Detection Systems ............................................................................................. 26

6.6 Monitoring Controls ............................................................................................................. 28

6.7 End-point security ................................................................................................................ 29
6.8 Wireless Security threats and Risk Mitigation .................................................................30
6.9 Voice-over IP .........................................................................................................................32
  6.9.1 Security Threats to VOIP ...............................................................................................33
  6.9.2 VOIP Security ..................................................................................................................33
6.10 Penetration Testing ..............................................................................................................33
  6.10.1 Types of Penetration Testing .........................................................................................35
  6.10.2 Risks associated with Penetration Testing .................................................................36
6.11 Auditing Network Security ..................................................................................................40
6.12 Summary .............................................................................................................................42
6.13 Questions ..............................................................................................................................43
6.14 Answers and Explanations .................................................................................................45
6.15 References ...........................................................................................................................46
  a. Publication: .........................................................................................................................46
  b. Websites: ..............................................................................................................................46
6.1 Introduction

We have seen the use of networks for business communication and application hosting in Module 1, in this section, we will review the risks and controls that are specific to networked computers. It is rare these days to find a standalone computer in any commercial environment, as networks offer tremendous advantages that far outweigh the cost of creating them. Although it is true that when we are implementing security controls it is necessary to focus on enterprise architecture as a whole for designing and implementing controls, network related controls are important since it is the first layer of architecture that is generally is focus of attacker. Therefore networks are also far more vulnerable to external and internal threats than are standalone systems.

Organization level general controls like physical security (cables, intruders trying to connect to network), environmental security (ensuring segregation between electrical and data cables, protecting cables from rodents), access controls, security policies (acceptable usage of internet) are applicable to network security. In addition one needs to look at network specific controls to ensure that organization’s security objectives are achieved.

6.2 Network Characteristics

Advantages of enterprise wide network characteristics are described as the following:

- **Anonymity**: A network removes personal interaction i.e. most of the clues, such as appearance, voice, or context, by which we recognize acquaintances.
- **Automation**: In some networks, one or both endpoints, as well as all intermediate points, involved in a given communication may be machines with only minimal human supervision.
- **Distance**: Many networks connect endpoints that are physically far apart. Although not all network connections involve distance, the speed of communication is fast enough that humans usually cannot tell whether a remote site is near or far. Though it makes it easier to establish communication among geographically dispersed users/machines, it also introduces risks like impersonation, intrusion, tapping.
- **Opaqueness**: Because the dimension of distance is hidden, users cannot tell whether a remote host is in the room next door or in a different country. In the same way, users cannot distinguish whether they are connected to a node in an office, school, home, or warehouse,
or whether the node’s computing system is large or small, modest or powerful. In fact, users cannot tell if the current communication involves the same machine with which they communicated the last time.

- **Routing diversity**: To maintain or improve reliability and performance, routings between two endpoints are usually dynamic. That is, the same interaction may follow one path through the network the first time and a very different path the second time. In fact, a query may take a different path from the response that follows a few seconds later.

### 6.3 Threats and Vulnerabilities

This section describes the various kinds of vulnerabilities and threats associated with networks that aim to compromise the confidentiality, integrity, or availability of data, software and hardware by accidents, non-malicious humans, and malicious attackers. The threats and vulnerabilities are listed under the following heads:

- Information Gathering
- Communication Subsystem Vulnerabilities
- Protocol Flaws
- Impersonation
- Message Confidentiality Threats
- Message Integrity Threats
- Web Site Defacement
- Denial of Service
However it needs to be understood that most of these threats operate in tandem and it is difficult to associate them with network security alone. Figure 6.1 illustrates the various threats in and their source or initiator. This will help auditors in understanding types of threat that might materialize in which part of IT installation and verify controls for those threats, based on risk assessment results.

6.3.1 Information Gathering

A serious attacker will spend a lot of time obtaining as much information as s/he can about the target before launching an attack. The techniques to gather information about the networks are examined below:

- **Port Scan**: An easy way to gather network information is to use a port scanner, a program that, for a particular IP address, reports which ports respond to messages and which of several known vulnerabilities seem to be present.

- **Social Engineering**: Social engineering involves using social skills and personal interaction to get someone to reveal security-relevant information and perhaps even to do something that permits an attack. The point of social engineering is to persuade the victim to be helpful. The attacker often impersonates someone occupying a senior position inside the organization and is in some difficulty. The victim provides the necessary assistance without verifying the identity of the caller, thus compromising security.
- **Reconnaissance**: Reconnaissance is the general term for collecting information. In security, it often refers to gathering discrete bits of information from various sources and then putting them together to make a coherent picture. One commonly used reconnaissance technique is “dumpster diving.” It involves looking through items that have been discarded in garbage bins or waste paper baskets. One might find network diagrams, printouts of security device configurations, system designs and source code, telephone and employee lists, and more. Even outdated printouts may be useful. Reconnaissance may also involve eavesdropping. The attacker or his accomplice may follow employees to lunch and listen in from nearby tables as co-workers discuss security matters.

- **Operating System and Application Fingerprinting**: Here the attacker wants to know which commercial server application is running, what version, and what the underlying operating system and version are. While the network protocols are standard and vendor independent, each vendor has implemented the standard independently, so there may be minor variations in interpretation and behaviour. The variations do not make the software noncompliant with the standard, but they are different enough to make each version distinctive. How a system responds to a prompt (for instance, by acknowledging it, requesting retransmission, or ignoring it) can also reveal the system and version. New features also offer a clue, for example a new version will implement a new feature but an old version will reject the request. All these peculiarities, sometimes called the operating system or application fingerprint, can mark the manufacturer and version.

- **Bulletin Boards and Chats**: Underground bulletin boards and chat rooms support exchange of information among the hackers. Attackers can post their latest exploits and techniques, read what others have done, and search for additional information on systems, applications, or sites.

- **Documentation**: The vendors themselves sometimes distribute information that is useful to an attacker. For example, resource kits distributed by application vendors to other developers can also give attackers tools to use in investigating a product that can subsequently be the target of an attack.

- **Malware**: Attacker may use malware like virus or worms to scavenge the system and keep sending information to attacker over network without the knowledge of system user.

### 6.3.2 Exploiting communication subsystem vulnerabilities

- **Eavesdropping and Wiretapping**: An attacker can pick off the content of a communication passing in unencrypted form. The term eavesdrop implies overhearing without expending any extra effort. For example, an attacker (or a system administrator) is eavesdropping by monitoring all traffic passing through a node. (The administrator might have a legitimate purpose, such as watching for inappropriate use of resources.) A more hostile term is wiretap, which means intercepting communications through some effort. Passive wiretapping is just “listening,” just like eavesdropping. But active wiretapping means injecting something into the
A wiretap can be done in such a manner that neither the sender nor the receiver of a communication will know that the contents have been intercepted.

- **Microwave signal tapping**: Microwave signals are broadcast through the air, making them more accessible to outsiders. An attacker can intercept a microwave transmission by interfering with the line of sight between sender and receiver. It is also possible to pick up the signal from an antenna located close to the legitimate antenna.

- **Satellite Signal Interception**: In satellite communication, the potential for interception is even greater than with microwave signals. However, because satellite communications are heavily multiplexed, the cost of extracting a single communication is rather high.

- **Wireless**: Wireless networking is becoming very popular, but threats arise in the ability of intruders to intercept and spoof a connection. A wireless signal is strong for approximately 30 to 60 meters. A strong signal can be picked up easily. Wireless also has a second problem, the possibility of unauthorized use of a network connection, or a theft of service.

- **Optical Fiber**: It is not possible to tap an optical system without detection. Further optical fiber carries light energy, not electricity, which does not emanate a magnetic field as electricity docs. Therefore, an inductive tap is impossible on an optical fiber cable. However, the repeaters, splices, and taps along a cable are places at which data may be intercepted more easily than in the fiber cable itself.

- **Zombies and BOTnet**: BOTnets is a term (robotic network) used for virtual network of zombies. BOTnet operator launches malware/virus on system that once activated remains on system and can be activated remotely. This malware helps the BOTnet operator use the compromised system (Zombie) remotely with to launch attack or collect information. For example Zombies have been used extensively to send e-mail spam. This allows spammers to avoid detection and presumably reduces their bandwidth costs, since the owners of zombies pay for their own bandwidth.

### 6.3.3 Protocol Flaws

Internet protocols are publicly posted for scrutiny. Many problems with protocols have been identified by reviewers and corrected before the protocol was established as a standard. Despite this process of peer review, flaws exist in many of the commonly used protocols. These flaws can be exploited by an attacker. For example FTP is known to transmit communication including user id and password in plain text.

### 6.3.4 Impersonation

In many instances, an easy way to obtain information about a network is to impersonate another person or process. An impersonator may foil authentication by any of the following means:
- **Authentication foiled by guessing:** Guess the identity and authentication details of the target, by using common passwords, the words in a dictionary, variations of the user name, default passwords, etc.
- **Authentication foiled by eavesdropping or wiretapping:** When the account and authentication details are passed on the network without encryption, they are exposed to anyone observing the communication on the network. These authentication details can be reused by an impersonator until they are changed.
- **Authentication Foiled by Avoidance:** A flawed operating system may be such that the buffer for typed characters in a password is of fixed size, counting all characters typed, including backspaces for correction. If a user types more characters than the buffer would hold, the overflow causes the operating system to bypass password comparison and act as if a correct authentication has been supplied. Such flaws or weaknesses can be exploited by anyone seeking unauthorized access.
- **Non-existent Authentication:** Here the attacker circumvents or disables the authentication mechanism at the target computer. If two computers trusts each other’s authentication an attacker may obtain access to one system through an authentication weakness (such as a guest password) and then transfer to another system that accepts the authenticity of a user who comes from a system on its trusted list. The attacker may also use a system that has some identities requiring no authentication. For example, some systems have “guest” or “anonymous” accounts to allow outsiders to access things the systems want to release to the public. These accounts allow access to unauthenticated users.
- **Well-Known Authentication:** Most vendors often sell computers with one system administration account installed, having a default password. Or the systems come with a demonstration or test account, with no required password. Some administrators fail to change the passwords or delete these accounts, creating vulnerability.
- **Spoofing and Masquerading:** Both of them are impersonation. Refer to chapter on logical access controls for details.
- **Session Hijacking:** Session hijacking is intercepting and carrying on a session begun by another entity. In this case the attacker intercepts the session of one of the two entities that have entered into a session and carry it over in the name of that entity. For example, in an e-commerce transaction, just before a user places his order and gives his address, credit number etc. the session could be hijacked by an attacker.
- **Man-in-the-Middle Attack:** A man-in-the-middle attack is a similar to session hijacking, in which one entity intrudes between two others. The difference between man-in-the-middle and hijacking is that a man-in-the-middle usually participates from the start of the session, whereas a session hijacking occurs after a session has been established. The difference is largely semantic and not particularly significant.
6.3.5 Message Confidentiality Threats

An attacker can easily violate message confidentiality (and perhaps integrity) because of the public nature of networks. Eavesdropping and impersonation attacks can lead to a confidentiality or integrity failure. Here we consider several other vulnerabilities that can affect confidentiality.

- **Mis-delivery**: Message mis-delivery happens mainly due to congestion at network elements which causes buffers to overflow and packets dropped. Sometimes messages are mis-delivered because of some flaw in the network hardware or software. Most frequently, messages are lost entirely, which is an integrity or availability issue. Occasionally, however, a destination address will be modified or some router or protocol will malfunction, causing a message to be delivered to someone other than the intended recipient. All of these “random” events are quite uncommon. More frequent than network flaws are human errors, caused by mistyping an address.

- **Exposure**: The content of a message may be exposed in temporary buffers, at switches, routers, gateways, and intermediate hosts throughout the network; and in the workspaces of processes that build, format, and present the message. A malicious attacker can use any of these exposures as part of a general or focused attack on message confidentiality.

- **Traffic Analysis (or Traffic Flow Analysis)**: Sometimes not only is the message itself sensitive but the fact that a message exists is also sensitive. For example, if a wartime enemy sees a large amount of network traffic between headquarters and a particular unit, the enemy may be able to infer that significant action is being planned involving that unit. In a commercial setting, messages sent from the president of one company to the president of a competitor could lead to speculation about a takeover or conspiracy to fix prices.

6.3.6 Message Integrity Threats

In most cases, the integrity or correctness of a communication is more important than its confidentiality. Some of the threats which could compromise integrity are by:

- Changing some or all of the content of a message
- Replacing a message entirely, including the date, time, and sender/receiver identification
- Reusing (replaying) an old message
- Combining pieces of different messages into one false message
- Changing the apparent source of a message
- Redirecting a message
- Destroying or deleting a message

These attacks can be perpetrated in the ways already stated, including:
6.3.7 Web Site Defacement

Web site defacement is common not only because of its visibility but also because of the ease with which one can be done. Web sites are designed so that their code is downloaded and executed in the client (browser). This enables an attacker to obtain the full hypertext document and all programs and references programs embedded in the browser. This essentially gives the attacker the information necessary to attack the web site. Most websites have quite a few common and well known vulnerabilities that an attacker can exploit.

6.3.8 Denial of Service

Denial of Service (DoS) attacks lead to loss of network availability. The electronic threats are more serious and less obvious. Some of them are described below:

- **Connection Flooding:** This is the oldest type of attack where an attacker sends more data than what a communication system can handle, thereby preventing the system from receiving any other legitimate data. Even if an occasional legitimate packet reaches the system, communication will be seriously degraded.
- **Ping of death:** It is possible to crash, reboot or otherwise kill a large number of systems by sending a ping of a certain size from a remote machine. This is a serious problem, mainly because this can be reproduced very easily, and from a remote machine. Ping is an ICMP protocol which requests a destination to return a reply, intended to show that the destination system is reachable and functioning. Since ping requires the recipient to respond to the ping request, all the attacker needs to do is send a flood of pings to the intended victim.
- **Traffic Redirection:** A router is a device that forwards traffic on its way through intermediate networks between a source host’s network and a destination’s. So if an attacker can corrupt the routing, traffic can disappear.
- **DNS Attacks:** DNS attacks are actually a class of attacks based on the concept of domain name server. A domain name server (DNS) is a table that converts domain names like www.icai.org into network addresses like 202.54.74.130, a process called resolving the domain name or name resolution. By corrupting a name server or causing it to cache spurious entries, an attacker can redirect the routing of any traffic, or ensure that packets intended for a particular host never reach their destination.
6.3.9 Distributed Denial of Service

In distributed denial of service (DDoS) attack more than one machine are used by the attacker to attack the target. These multiple machines are called zombies that act on the direction of the attacker and they don't belong to the attacker. These machines have some vulnerability that can be exploited to use it to attack another machine. The attacker exploits vulnerabilities in multiple machines and uses them to attack the target simultaneously. In addition to their tremendous multiplying effect, distributed denial-of-service attacks are a serious problem because they are easily launched by using scripts.

6.3.10 Threats from Cookies, Scripts and Active or Mobile Code

Some of the vulnerabilities relating to data or programs that are downloaded from the server and used by the client are as follows:

- **Cookies**: Cookies are NOT executable. They are data files created by the server that can be stored on the client machine and fetched by a remote server usually containing information about the user on the client machine. Anyone intercepting or retrieving a cookie can impersonate the cookie’s legitimate owner.

- **Scripts**: Clients can invoke services by executing scripts on servers. A malicious user can monitor the communication between a browser and a server to see how changing a web page entry affects what the browser sends and then how the server reacts. With this knowledge, the malicious user can manipulate the server’s actions. The common scripting languages for web servers, CGI (Common Gateway Interface), and Microsoft’s active server pages (ASP) have vulnerabilities that can be exploited by an attacker.

- **Active Code**: Active code or mobile code is a general name for code that is downloaded from the server by the client and executed on the client machine. The popular types of active code languages are Java, JavaScript, VBScript and ActiveX controls. Such executable code is also called applet. A hostile applet is downloadable code that can cause harm on the client’s system. Because an applet is not screened for safety when it is downloaded and because it typically runs with the privileges of its invoking user, a hostile applet can cause serious damage.

6.3.11 Malicious Code

Malicious code is the name used for any program that adds to, deletes or modifies legitimate software for the purpose of intentionally causing disruption and harm or to circumvent or subvert the existing system’s function. Examples of malicious code include viruses, worms, Trojan Horses, and logic bombs. Newer malicious code is based on mobile Active X and Java applets.
Viruses

A computer virus is a type of malware (program) that attaches itself to a file and gets transmitted. When executed, it damages the infected system and also replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected".

Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, or logging their keystrokes. However, not all viruses carry a destructive payload or attempt to hide themselves—the defining characteristic of viruses is that they are self-replicating computer programs which install themselves without the user's consent.

Motives for creating viruses can include seeking profit; desire to send a political message, personal amusement, to demonstrate that vulnerability exists in software, for sabotage and denial of service.

Viruses often are classified based on the type of damage they do when infected. The major types are:

a. **Master Boot Record (MBR) Viruses**: Affects the boot sector of storage device and further infects when the storage is accessed.

b. **Stealth Viruses**: Stealth viruses hide themselves by tampering the operating system to fool antivirus software into thinking that everything is functioning normally.

c. **Polymorphic Viruses**: Polymorphic viruses are difficult to detect because they can modify themselves and change their identity thus able to hide themselves from antivirus software.

d. **Macro Viruses**: Macro viruses are the most prevalent computer viruses and can easily infect many types of applications, such as Microsoft Excel and Word.

e. **Worms**: Worms are stand-alone viruses that are they are transmitted independently and executes themselves.

f. **Trojan horse**: Malicious code hidden under legitimate program, such as a game or simple utility. Trojans are primarily used by attackers to infect the system and then get control remotely to make that system work for them.

**Logic Bomb/Time Bomb**

Logic bombs are malicious code added to an existing application to be executed at a later date. These can be intentional or unintentional. For example Year2000 problem was an unintentional logic bomb. Every time the infected application is run, the logic bomb checks the date to see whether it is time to run the bomb. If not, control is passed back to the main application and the
logic bomb waits. If the date condition is correct, the rest of the logic bomb’s code is executed and the result can be anything from a harmless message to a system crash.

6.3.12 Virus / Malicious Code protection mechanisms:

Various countermeasures that can be deployed to protect against virus are:

a) **Anti-Virus**: Antivirus is most common protection from virus and is installed on most of laptops and desktops. Most of the antivirus software utilizes a method known as signature detection to identify potential virus infections on a system. Essentially, they maintain an extremely large database that contains the known characteristics (signatures) of all viruses. Depending upon the antivirus package and configuration settings, it can scan storage media periodically, check for any files that contain data matching those criteria. Antivirus tools have three types of controls –
   - Active monitor: Monitors traffic and activity to check the viruses. Although most tools use signatures, few have developed heuristic scan abilities to look for possible malicious codes
   - Repair or quarantine: These tools tries to remove the virus from file/mail or quarantines and reports.
   - Scheduled scan: Users are prompted for scanning the storages to detect virus already present, that were not detected by active monitors. This happen when the new virus enters the system. (Zero day attack)

   It is essential to ensure following controls:
   - Virus signatures are updated
   - Alerts from antivirus are reviewed for root cause
   - Schedules scans are performed regularly

b) **Incident handling**: Incident Handling is an action plan for dealing with virus attack, intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. It is comprised of a six step process: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned. In case of virus incidents it is most essential to find out root cause to ensure that the incident does not recur.

c) **Training and Awareness programs**: It is said that human beings are the weakest link in information security. Periodic training and awareness programs need to be organized to ensure that employees and other 3rd party users are made aware of the risks arising out of improper use of organisation’s information systems. These cover:
   - Enforcing policy on use of removable devices
   - Handling of mail attachments particularly from unknown senders
   - Accessing internet
   - Ensuring antivirus is updated and scheduled scan are performed (generally it is automated and centralized)
6.4 Current Trends in attacks

Most attacks and threats discussed above are being in use for a considerable time. Organizations being aware of their existence mostly ensure that controls are in place to prevent, detect and/or recover from these attacks. However attackers are always a step ahead. Attackers are now using other means to attack some of these are discussed below.

6.4.1 Exploiting application vulnerabilities

With use of internet based technologies and clouds organizations have hosted applications that can be accessed from internet and/or intranet. These applications might contain vulnerabilities if exploited can compromise the security of information. Attackers tried to exploit these vulnerabilities to launch the attacks like SQL Injection, Cross site scripting. OWASP (Open web application Security project) identifies top ten security threats every years. Threats identified in 2013 are listed below. (Source: www.owasp.org)

- **Injection (SQL Injection)**: Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker’s hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
- **Broken Authentication and Session Management**: Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users’ identities.
- **Cross-Site Scripting (XSS)**: XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim’s browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
- **Insecure Direct Object References**: A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
- **Security Misconfiguration**: Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.
- **Sensitive Data Exposure**: Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.
Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

- **Missing Function Level Access Control**: Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

- **Cross-Site Request Forgery (CSRF)**: A CSRF attack forces a logged-on victim’s browser to send a forged HTTP request, including the victim’s session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim’s browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

- **Using Components with Known Vulnerabilities**: Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defences and enable a range of possible attacks and impacts.

- **Invalidated Redirects and Forwards**: Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

### 6.4.2 Advanced persistent threat (APT)

A sustained targeted attack on identified subject. Attacker tried to introduce malware to compromise the system. For this attacker uses possible social engineering methods. Once the system is compromises the malware resides in system. Since malware is specifically written antivirus may not be able to detect it. This malware is designed to send small bits of information from system to attacker without getting detected by network based controls like anomaly detection, traffic analysis etc. The attack continues for a longer duration till all required confidential information about organization is received by the attacker.

### 6.5 Network Security Controls

This section examines controls available to ensure network security from the various threat identified listed earlier. The controls are listed under the following broad heads.

- Architecture
- Cryptography/Encryption
- Content Integrity
Module 4

- Strong Authentication
- Remote Access Security
- Firewalls
- Intrusion Detection Systems
- Monitoring (Security Incident and Event Management (SIEM))

6.5.1 Architecture

The architecture or design of a network can have a significant effect on its security. Some of the major considerations are:

- **Segmentation / Zoning:** Segmentation / Zoning can limit the potential for harm in a network in two important ways. Segmentation reduces the number of threats, and it limits the amount of damage a single vulnerability can allow. A web server, authentication server, applications and database are residing on a single server or segment for facilitating electronic commerce transactions are a very insecure configuration. A more secure design will use multiple segments. Since the web server has to be exposed to the public, that server should not have other more sensitive, functions on it or residing on the same segment such as user authentication or access to the database. Separate segments and servers reduce the potential harm should any subsystem be compromised. (Please see figure 6.2 in next page).

- **Redundancy:** Another key architectural control is redundancy, allowing a function to be performed on more than one node. Instead of having a single web server; a better design would have two servers, using a “failover mode”. If one server is used and that server is down for some reason the whole application is not available. In failover mode, the servers communicate with each other periodically, each determining if the other is still active. If one fails, the other takes over processing for both of them. Although performance is cut approximately in half when a failure occurs, some minimum processing is being done which can be used to maintain critical functions.

- **Eliminate Single Points of Failure:** Good network architecture provides for its availability by eliminating single points of failure. This is true for all critical components including servers, network devices and communication channels in a network that will compromise its availability, if it fails.
6.5.2 Cryptography/Encryption

The technical details of cryptography have been dealt with in an earlier module. Only certain applications of cryptography that are relevant to Network security are discussed here.

Link Encryption

In link encryption, data are encrypted just before the system places them on the physical communications link, that is, encryption occurs at the Data Link layer in the OSI model. Correspondingly, decryption occurs at the Data Link layer of the receiving host. Link encryption protects the message in transit between two computers, but the message is in plaintext inside the hosts (above the data link layer). Headers added by the network layer (which includes addresses, routing information and protocol) and above are encrypted, along with the message/data. The message is, however, exposed at the Network layer and thus all intermediate nodes through which the message passes can read the message. This is because all routing and addressing is done at the Network layer. Link encryption is invisible to user and appropriate when the transmission line is the point of greatest vulnerability. Link encryption provides protection against traffic analysis.
End-to-End Encryption

End-to-end encryption provides security from one end of a transmission to the other. The encryption can be applied by a hardware device between the user and the host or the encryption can be done by software running on the host computer. In either case, the encryption is performed at the higher layers, usually application or presentation layer. When end-to-end encryption is used, messages, even when sent through several insecure intermediate hosts, are protected. This is because the data content remains encrypted at all the intermediate layers. However, since the
headers below the transport is not encrypted (networks, data link, etc.) end-to-end does not provide protection against traffic analysis. Note that it is possible use both Link and End-to-end encryption at the same time. One does not preclude the other.

Table 6.1: Comparison of Link and End-to-End Encryption

<table>
<thead>
<tr>
<th>Link Encryption</th>
<th>End-to-End Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security within hosts</td>
<td></td>
</tr>
<tr>
<td>Data exposed in sending host</td>
<td>Data encrypted in sending host</td>
</tr>
<tr>
<td>Data exposed in intermediate nodes</td>
<td>Data encrypted in intermediate nodes</td>
</tr>
<tr>
<td>Role of user</td>
<td></td>
</tr>
<tr>
<td>Applied by sending host</td>
<td>Applied by sending process</td>
</tr>
<tr>
<td>Invisible to user</td>
<td>User applies encryption</td>
</tr>
<tr>
<td>Host maintains encryption</td>
<td>User must find algorithm</td>
</tr>
<tr>
<td>One facility for all users</td>
<td>User selects encryption</td>
</tr>
<tr>
<td>Typically done in hardware</td>
<td>Either software or hardware implementation</td>
</tr>
<tr>
<td>All or no data encrypted</td>
<td>User chooses to encrypt or not, for each data item</td>
</tr>
<tr>
<td>Implementation concerns</td>
<td></td>
</tr>
<tr>
<td>Requires one key per host pair</td>
<td>Requires one key per user pair</td>
</tr>
<tr>
<td>Provides node authentication</td>
<td>Provides user authentication</td>
</tr>
</tbody>
</table>

PKI and Certificates

A public key infrastructure (PKI) is a process created to enable users to implement public key (asymmetric) cryptography, usually in a large and distributed setting. PKI offers each user a set of services, related to identification and access control, as follows:

- Create certificates associating a user's identity with a (public) cryptographic key
- Issue certificates from its database
- Sign certificates, adding its credibility to the authenticity of the certificate
- Confirm (or deny) the validity of a certificate
- Revoke certificates for users who no longer are allowed access or whose private key has been exposed

PKI is a set of policies, procedures and products and not a standard. The policies define the rules under which the cryptographic systems should operate. In particular, the policies specify how to handle keys and valuable information and how to match level of control to level of risk. The procedures dictate how the keys should be generated, managed, and used. Finally, the products
actually implement the policies, and they generate, store, and manage the keys. Entities, called certificate authorities, implement the PKI policy on certificates. The functions of a certificate authority can be done in-house or by a commercial service or a trusted third party. PKI may also involve a registration authority that acts as an interface between a user and a certificate authority. The registration authority captures and authenticates the identity of a user and then submits a certificate request to the appropriate certificate authority.

SSL Encryption
The SSL (Secure Sockets Layer) protocol was originally designed by Netscape to protect communication between a web browser and server. It is also known now as TLS, for transport layer security. SSL interfaces between applications (such as browsers) and the TCP/IP protocols to provide server authentication, optional client authentication, and an encrypted communications channel between client and server.

To create a SSL connection, the client requests an SSL session. The server responds with its public key certificate so that the client can determine the authenticity of the server. The client returns symmetric session key encrypted under the server’s public key. The server decrypts the session key and then they switch to encrypted communication, using the shared session key.

IPSec
IETF (Internet Engineering Task Force) adopted IPSec, or the IP Security Protocol Suite. Designed to address spoofing, eavesdropping, and session hijacking, the IPSec protocol defines a standard means for handling encrypted data. IPSec is implemented at the IP layer, so it affects all layers above it, in particular TCP and UDP.

IPSec is similar to SSL, in that it supports authentication and confidentiality in a way that does not necessitate significant change either above it (in applications) or below it (in the TCP protocols). Like SSL, it was designed to be independent of specific cryptographic protocols and to allow the two communicating parties to agree on a mutually supported set of protocols.

<table>
<thead>
<tr>
<th>Physical Header</th>
<th>IP Header</th>
<th>TCP Header</th>
<th>Data</th>
<th>Physical Trailer</th>
</tr>
</thead>
</table>

Figure 6.5: Traditional Packets
Signed Code
As already noted, it is possible for someone to place malicious active code on a web site to be downloaded by unsuspecting users. A partial solution to reduce this risk is to use signed code. A trustworthy third party appends a digital signature to a piece of code (or macro), supposedly connoting more trustworthy code. A signature structure in a PKI helps to validate the signature. A well-known manufacturer would be recognizable as a code signer.

Encrypted E-Mail
An electronic mail message generally has no privacy at all. The service provider and any intermediate host can read not just the address but also everything in the message field. To protect the privacy of the message and routing information, we need encryption to protect the confidentiality and integrity of the message. The two popular approaches to key management are using a hierarchical, certificate based PKI solution for key exchange and using a flat, individual-to-individual exchange method. The hierarchical method is called S/MIME (Secure Multi-Purpose Mail Extensions) and is employed by many commercial mail programs, such as Microsoft Exchange. The individual method is called PGP (Pretty Good Privacy) and is a commercial add-on.

6.5.3 Content Integrity
Content integrity is automatically implied when cryptographic systems are used. Most kinds of malicious threats are addressed by cryptographic systems very effectively. For non-malicious threats to integrity, the controls are Error Correcting codes and Message Digests (Cryptographic Checksums)

Error Correcting Codes
Error detection codes detect when an error has occurred, and error correction codes can actually correct errors without requiring retransmission of the original message. The error code is transmitted along with the original data, so the recipient can re-compute the error code and check whether the received result matches the expected value.
• **Parity Check:** The simplest error detection code is a parity check. An extra bit (the parity bit) is added to an existing group of data bits depending on their sum. With even parity the extra bit is 0 if the sum of the data bits is even and 1 if the sum is odd; that is, the parity bit is set so that the sum of all data bits plus the parity bit is even. Odd parity is the same except the sum is odd. Parity bits are useful only when the error is in a single bit (called single bit error).

• **Checksum and CRCs:** A checksum is a form of redundancy check that at its simplest, works by adding up the basic components of a message, usually the bits or bytes, and storing the resulting value. Later, anyone who has the authentic checksum can verify that the message was not corrupted by doing the same operation on the data, and checking the sum. A more sophisticated type of redundancy check is the cyclic redundancy checks (CRC) which considers not only the value of each bit/byte but also the order of the values. A cyclic redundancy check (CRC) uses a hash function used to produce a checksum which is a small integer from a large block of data, such as network traffic or computer files, in order to detect errors in transmission or duplication. CRCs are calculated before and after transmission or duplication, and compared to confirm that they are the same.

• **Other Codes:** Other kinds of error detection codes, such as hash codes and Hamming codes are used to detect burst errors (several errors occurring contiguously) and multiple bit errors (multiple errors among non-adjacent bits). Some of the more complex codes (like Hamming codes) can detect multiple-bit errors and may be able to pinpoint which bits have been changed, thus allowing the data to be corrected.

**Message Digests (Cryptographic Checksums)**

Checksums and CRCs are useful in detecting accidental modification such as corruption to stored data or errors in a communication channel. However, they provide no security against malicious agents, as their simple mathematical structure makes them trivial to circumvent. To protect against malicious changes cryptographic checksum are used. A cryptographic checksum is created by performing a complicated series of mathematical operations (the cryptographic algorithm) that translates the data in the file into a fixed string of digits called a hash value, which is then used as a checksum. Without knowing which cryptographic algorithm was used to create the hash value, it is highly unlikely that an unauthorized person would be able to change data without inadvertently changing the corresponding checksum.

A cryptographic hash function must ensure that the following is computationally infeasible:

- Determining the content of a message from its Cryptographic Checksums
- Finding “collisions”, wherein two different messages have the same Cryptographic Checksums.

Cryptographic checksums are also known as message digests, message authentication codes, integrity check-values, modification detection codes, or message integrity codes.
6.5.4 Strong Authentication

A security policy specifies who—which individuals, groups, subjects can access which resources and objects. Crucial to that policy is authentication: knowing and being assured of the accuracy of identities. Organization must adopt strong authentication methods appropriate for use in networks like one-time passwords, Challenge Response systems and Kerberos, discussed in previous chapter.

6.5.5 Remote Access Security

Remote access technologies can be defined as those data networking technologies that are focused on providing the remote user with access into a network, while striving to maintain the principal tenets of Confidentiality, Availability, and Integrity. There are many obvious advantages to employing secure remote network access, such as the following:

- Reducing networking costs by using the Internet to replace expensive dedicated network lines
- Providing employees with flexible work styles such as telecommuting
- Building more efficient ties with customers, suppliers, and employees

Virtual Private Networking (VPN)

A virtual private network (VPN) is created by building a secure communications link between two nodes by emulating the properties of a point-to-point private link. A VPN can be used to facilitate secure remote access into a network, securely connect two networks together, or create a secure data tunnel within a network. Encryption coupled with access controls (including firewalls) can provide users with the same level of privacy that can be provided on a private network, even when
the communication traverses a part of the public network. For more details, refer the previous module.

**Figure 6.7: Secure VPN**

**Dial back procedures**

In a networked computing environment, user may often require access to the systems resources from remote locations. Dial-back systems are a control to ensure that access is made only from authorized lines or locations. When a user dials into the server and identifies itself, the server hangs up and calls the user at a pre-determined telephone number and then enables the user to access the resources based on password authentication. A weakness in this procedure is call-forwarding. An unauthorized person could enable calls to a pre-determined number to be forwarded to the number designated by him, thus enabling him to gain unauthorized access to the resources.

**Other controls**

To minimize the risk of unauthorized dial-in access, remote users should never store their passwords in plain text login scripts on notebooks and laptops.

**Authentication Servers**

In widely spread out networked systems, the problem of user management and enabling authorized access is crucial since users are spread over a wide geographical areas including telecommuting. In such cases all access control is transferred to a centralized or decentralized access authentication mechanism. Two of the popular applications of remote authentication mechanisms depending on centralized/decentralized access authentication implementations are TACACS (Terminal Access Controller Access Control System) and RADIUS (Remote Authentication Dial in User Service). Some of the features of such systems are:

- Enable secure remote access
- Facilitates centralized user management
- Facilitates centralized access monitoring and control
- Changes to user access rights made easy
- Provides event logging and extended audit trails

**6.5.6 Firewalls**

The technical details of firewalls, their types and configurations have been dealt with in the first module. Only certain specialised applications of firewalls for network security are dealt with here.
Intranet
An intranet is a network that employs the same types of services, applications, and protocols present in an Internet implementation, without involving external connectivity. For example, an enterprise network employing the TCP/IP protocol suite, along with HTTP for information dissemination would be considered an Intranet. Most organizations currently employ some type of intranet, although they may not refer to the network as such. Within the internal network (intranet), many smaller intranets can be created by the use of internal firewalls. As an example, an organization may protect its personnel network with an internal firewall, and the resultant protected network may be referred to as the personnel intranet. Since intranets utilize the same protocols and application services present on the Internet, many of the security issues inherent in Internet implementations are also present in intranet implementations. Therefore, intranets are typically implemented behind firewall environments.

Extranets
An extranet is usually a business-to-business intranet; that is, two intranets are joined via the Internet. The extranet allows limited, controlled access to remote users via some form of authentication and encryption such as provided by a VPN. Extranets share nearly all of the characteristics of intranets, except that extranets are designed to exist outside a firewall environment. By definition, the purpose of an extranet is to provide access to potentially sensitive information to specific remote users or organizations, but at the same time denying access to general external users and systems. Extranets employ TCP/IP protocols, along with the same standard applications and services. Many organizations and agencies currently employ extranets to communicate with clients and customers. Within an extranet, options are available to enforce varying degrees of authentication, logging, and encryption.

Securing a Firewall
Firewall platforms should be implemented on systems containing operating system builds that have been stripped down and hardened for security applications. Firewalls should never be placed on systems built with all possible installation options. Firewall operating system builds should be based upon minimal feature sets. All unnecessary operating system features should be removed from the build prior to firewall implementation. All appropriate operating system patches should be applied before any installation of firewall components.

The operating system build should not rely strictly on modifications made by the firewall installation process. Firewall installation programs rely on a lowest common denominator approach; extraneous software packages or modules might not be removed or disabled during the installation process.
The hardening procedure used during installation should be tailored to the specific operating system undergoing hardening. Some often-overlooked issues include the following:

- Any unused networking protocols should be removed from the firewall operating system build. Unused networking protocols can potentially be used to bypass or damage the firewall environment. Finally, disabling unused protocols ensures that attacks on the firewall utilizing protocol encapsulation techniques will not be effective.
- Any unused network services or applications should be removed or disabled. Unused applications are often used to attack firewalls because many administrators neglect to implement default-restrictive firewall access controls. In addition, unused network services and applications are likely to run using default configurations, which are usually much less secure than production-ready application or service configurations.
- Any unused user or system accounts should be removed or disabled. This particular issue is operating system specific, since all operating systems vary in terms of which accounts are present by default as well as how accounts can be removed or disabled.
- Applying all relevant operating system patches is also critical. Since patches and hot fixes are normally released to address security-related issues, they should be integrated into the firewall build process. Patches should always be tested on a non-production system prior to rollout to any production systems.
- Unused physical network interfaces should be disabled or removed from the server chassis.

6.5.7 Intrusion Detection Systems

After the perimeter controls, firewall, and authentication and access controls block certain actions, some users are admitted to use a computing system. Most of these controls are preventive, that is, they prevent known undesirable things from happening. Many studies, however, have shown that most computer security incidents are caused by insiders, people who would not be blocked by a firewall. And insiders require access with significant privileges to do their daily jobs.

Intrusion detection systems complement these preventive controls as the next line of defence. An intrusion detection system (IDS) is a device, usually another separate computer, which monitors activity to identify malicious or suspicious events. An IDS is a sensor that raises an alarm if specific things occur. The alarm can range from writing an entry in an audit log, to something significant, such as paging the system security administrator. An IDS receives inputs from sensors. It saves those inputs, analyses them, and takes some controlling action.

The functions performed by IDS are:

- Monitoring users and system activity
- Auditing system configuration for vulnerabilities and mis-configurations
Network Security Controls

- Assessing the integrity of critical system and data files
- Recognizing known attack patterns in system activity
- Identifying abnormal activity through statistical analysis
- Managing audit trails and highlighting user violation of policy or normal activity
- Correcting system configuration errors
- Installing and operating traps to record information about intruders
- Special considerations in audit of remote access and network security

Many intrusion detection systems are also capable of interacting with firewalls in order to bring a reactive element to the provision of network security services. Firewalls that interact with intrusion detection systems are capable of responding to perceived remote threats automatically, without the delays associated with a human response. For example, if an intrusion detection system detects a denial of service attack in progress, it can instruct certain firewalls to automatically block the source of the attack (although, false positives responses can occur).

The two general types of intrusion detection systems are signature based and heuristic. Signature-based intrusion detection systems perform simple pattern-matching and report situations that match a pattern corresponding to a known attack type. Heuristic intrusion detection systems, also known as anomaly based, build a model of acceptable behaviour and flag exceptions to that model; for the future, the administrator can mark a flagged behaviour as acceptable so that the heuristic IDS will now treat that previously unclassified behaviour as acceptable.

Intrusion detection devices can be network based or host based. A network-based IDS is a stand-alone device attached to the network to monitor traffic throughout that network; a host-based IDS runs on a single workstation or client or host, to protect that one host. For more details, please see the previous module.
6.6 Monitoring Controls
Most controls implemented for network generates lot of logs related to activities as per rule set. Monitoring and reviewing these logs is a mammoth task and need lot of efforts and resources. There are various tools available in market that helps organizations in collecting these logs, correlating them based on possible use cases and generate alerts for important logs. This way the efforts can be minimized but cannot be eliminated. Also resources required to manage these tools are specially trained and skilled. These tools are known as Security Incident and event management (SIEM) tools. Organizations use these tools and establish a security operations center (SOC) to monitor these logs, analyse alerts and record incidents and events to be responded. Broad Objectives of SOC are:

- Detect attacks and malware
- Enhance incident response capability
- Detect Advanced persistent threats
- Compliance requirements

A typical SOC is connected with other systems as shown in figure 6.9 given here.
Establishing SOC requires huge cost and resources and small organizations may prefer to outsource such services to vendor.

### 6.7 End-point security

In network security, endpoint security refers to a methodology of protecting the corporate network when accessed via remote devices such as laptops or other wireless and mobile devices. Each device with a remote connection to the network creates a potential entry point for security threats. Endpoint security is designed to secure each such access from the endpoint (device) to the network resources.
Figure 6.10: Typical wireless network

Usually, endpoint security is a security system that consists of security software, located on a centrally managed and accessible server or gateway within the network, in addition to client software being installed on each of the endpoints (or devices). The server authenticates logins from the endpoints and also updates the device software when needed. As an end-point wants to make an access to the network, the server software authenticates the device (i.e. the end point) and checks whether it conforms to the security policy of the organization before allowing the access. While endpoint security software differs by vendor, you can expect most software offerings to provide antivirus, antispyware, personal firewall and also a host intrusion prevention system.

Endpoint security is becoming a more common IT security function and concern as more employees bring consumer mobile devices to work and companies allow its mobile workforce to use these devices on the corporate network.

6.8 Wireless Security threats and Risk Mitigation

A wireless network is a type of computer network that uses wireless data connections for connecting network nodes. It is a method by which enterprise (office), homes, etc. avoid the costly process of introducing cables into a building, or as a connection between various equipment locations.
Wireless networking presents many advantages like network configuration and reconfiguration is easier, faster, and less expensive. However, wireless technology also creates new threats and alters the existing information security risk profile. For example, because communication takes place "through the air" using radio frequencies, the risk of interception is greater than with wired networks. If the message is not encrypted, or encrypted with a weak algorithm, the attacker can intercept and read it, thereby compromising confidentiality.

Wireless network has numerous vulnerabilities such as:

- **Ad-hoc networks**: Ad-hoc networks can pose a security threat. Ad-hoc networks are defined as peer-to-peer networks between wireless computers that do not have an access point in between them.

- **Non-traditional networks**: Non-traditional networks such as personal network Bluetooth devices are not safe from cracking and should be regarded as a security risk. Even barcode readers, handheld PDAs, and wireless printers and copiers should be secured. These non-traditional networks are commonly overlooked by IT personnel who have narrowly focused on laptops and access points.

- **MAC spoofing**: MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device. The MAC address is hard-coded on a network interface card (NIC) and cannot be changed. However, there are tools which can make an operating system believe that the NIC has a MAC address different that it’s real MAC address.

- **Man-in-the-middle attacks**: A man-in-the-middle attack is an attack in which an attacker secretly intercepts the electronic messages going between the sender and the receiver and then capture, insert and modify messages during message transmission.

- **Accidental association**: Unauthorized access to organisation’s wireless and wired networks can come from a number of different methods and intents. One of these methods is referred to as “accidental association”. When a user turns on a computer and it latches on to a wireless access point from a neighbouring organisation’s overlapping network, the user may not even know that this has occurred. However, it is a security breach in that proprietary organisation information is exposed and now there could exist a link from one organisation to the other. This is especially true if the laptop is also hooked to a wired network.

- **Denial of service**: It is an attempt to make a machine not available to its intended user.

Wireless network provides numerous opportunities to increase productivity and manage costs. Although it is impossible to totally eliminate all risks associated with wireless networking, it is possible to achieve a reasonable level of security by adopting a systematic approach to assessing and managing risk. Most common controls which are implemented in wireless environment are:
• **Encryption:** The best method for protecting the confidentiality of information transmitted over wireless networks is to encrypt all wireless traffic.

• **Signal-Hiding Techniques:** In order to intercept wireless transmissions, attackers first need to identify and locate wireless networks. There are, however, a number of steps that an organization can take to make it more difficult to locate their wireless access points. The easiest options include: Turning off the service set identifier (SSID) broadcasting by wireless access points and reducing signal strength to the lowest level that still provides requisite coverage. More effective, but also more costly methods for reducing or hiding signals include: using directional antennas to constrain signal emanations within desired areas of coverage or using signal emanation-shielding techniques, also referred to as TEMPEST to block emanation of wireless signals.

• **Anti-virus and anti-spyware software:** Computers on a wireless network need the same protections as any computer connected to the Internet. Install anti-virus and anti-spyware software, and keep them up-to-date. If your firewall was shipped in the “off” mode, turn it on.

• **Default passwords:** Wireless routers generally come with standard default password that allows you to set up and operate the router. These default passwords are also available on the web. So change the router password immediately after its installation.

• **MAC address:** Every computer that is able to communicate with a network is assigned its own unique Media Access Control (MAC) address. Wireless routers usually have a mechanism to allow only devices with particular MAC addresses access to the network.

### 6.9 Voice-over IP

Voice over Internet Protocol (VoIP) is a methodology for delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms commonly associated with VoIP are IP telephony, Internet telephony, voice over broadband (VoBB) and broadband telephony.

The term Internet telephony specifically refers to the provisioning of communications services (voice, fax, SMS, voice-messaging) over the public Internet, rather than via the public switched telephone network (PSTN). The steps and principals involved in originating VoIP telephone calls are similar to traditional digital telephony, and involve signalling, channel setup, digitization of the analog voice signals, and encoding. Instead of being transmitted over a circuit-switched network, however, the digital information is packetized and transmission occurs as Internet Protocol (IP) packets over a packet-switched network. VoIP is available on many smartphones, personal computers, and on Internet access devices. Calls and SMS text messages may be sent over 3G or Wi-Fi.
Network Security Controls

6.9.1 Security Threats to VOIP

VoIP systems rely on a data network, which means security weaknesses and the types of attacks associated with any data network are possible. For example, in a conventional telephone system, physical access to the telephone lines or a compromise of the office private branch exchange (PBX) is required for in order to conduct activities such as wire-tapping. But for VoIP, voice is converted into IP packets that may travel through many network access points. Therefore the data is exposed to many more possible points of attack that could be used for interception by intruders. In fact, all the security risks associated with IP, such as computer viruses, Denial of Service and man in the middle attacks, are also dangerous to VoIP systems. Most of the VoIP traffic over the Internet is not encrypted, so this traffic is exposed to the hackers. Hackers can intercept the communication or shut down the voice services by flooding servers (supporting VoIP) with bogus traffic.

6.9.2 VOIP Security

Encryption: Encryption is a means of preserving the confidentiality of transmitted signals.

- **Physical security**: Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to perform traffic analysis and derive call information from encrypted messages. Therefore, adequate physical security should be in place to restrict access to key VoIP network components.
- **Anti-virus and firewalls**: Computers which use software for VoIP connections should be protected with a personal firewall, along with anti-virus and anti-malicious code software that are up to date with the latest virus signature and/or malicious code definitions. This provides basic protection against attacks on the data segment that could be transferred to the voice segment.
- **Segregation of Voice and Data segments**: IP-based telephony provides a platform for telephone calls over an existing IP data network. However, in order to maintain quality of service (QoS), scalability, manageability, and security, voice and data should be separated using different logical networks as far as possible. Segmenting IP voice from a traditional IP data network greatly enhances the mitigation of VoIP attacks.

6.10 Penetration Testing

Penetration Testing is used by organizations to evaluate the effectiveness of information security implementation. As its name implies, penetration testing is a series of activities undertaken to identify and exploit security vulnerabilities. The idea is to find out how easy or difficult it might be
for someone to “penetrate” an organization’s security controls or to gain unauthorized access to its information and information systems.

A penetration test is performed by a team of experts. This team simulates attack using similar tools and techniques used by hackers. Penetration test cannot be expected to identify all possible security vulnerabilities because Penetration testing is conducted at a point in time. New technology, new hacker tools and changes to an organization’s information system can create exposures not anticipated during the penetration testing. Hence organizations perform these tests periodically.

Penetration Testing Scope

The scope of a penetration testing is to determine whether an organization’s security vulnerabilities can be exploited and its systems compromised. Conducting such a test involves gathering information about an organization’s information systems and information security and then using this information to attempt to identify and exploit known or potential security vulnerabilities. Evidence to support the penetration testing team’s ability to exploit security vulnerabilities can vary from gathering “computer screen shots” or copying sensitive information or files to being able to create new user accounts on the system or being able to create and/or delete particular files on the organization’s servers. Penetration testing can have a number of secondary objectives, including testing the security incident identification and response capability of the organization, testing employee security awareness or testing users’ compliance with security policies.

Penetration Testing Strategies

Various strategies for penetration testing, based on specific objectives to be achieved, include:

- **External vs. internal testing.** External testing refers to attacks on the organization’s network perimeter using procedures performed from outside the organization’s systems as they are visible to hacker. This can be a **Blind test** where testing expert has been provided with limited information.
- **Internal testing** is performed from within the organization’s technology environment. The focus is to understand what could happen if the network perimeter were successfully penetrated or what an authorized user could do to penetrate specific information resources within the organization’s network.
- **Targeted testing**: (often referred to as the “lights-turned-on” approach) involves both the organization’s IT team and the penetration testing team being aware of the testing activities and being provided information concerning the target and the network design.
A targeted testing approach may be more efficient and cost-effective when the objective of the test is focused more on the technical setting, or on the design of the network, than on the organization’s incident response and other operational procedures. A targeted test typically takes less time and effort to complete than blind testing, but may not provide as complete a picture security vulnerabilities and response capabilities of the organization.

6.10.1 Types of Penetration Testing

In addition to the penetration testing strategies to be used, consideration should be given to the types of testing the testing team is to carry out. These could include:

- **Application security testing**: Many organizations offer access to core business functionality through web-based applications. This type of access introduces new security vulnerabilities, because even with a firewall and other monitoring systems, security can be compromised, since traffic must be allowed to pass through the firewall. The objective of application security testing is to evaluate the controls over the application and its process flow. Areas of evaluation may include the application’s usage of encryption to protect the confidentiality and integrity of information, how users are authenticated, integrity of the Internet user’s session with the host application, and use of cookies – a block of data stored on a customer’s computer that is used by the web server application.

- **Denial of Service (DoS) testing**: The goal of DoS testing is to evaluate the system’s susceptibility to attacks that will render it inoperable so that it will “deny service,” that is, drop or deny legitimate access attempts. Decisions regarding the extent of Denial of Service testing to be incorporated into a penetration testing exercise will depend on the relative importance of ongoing, continued availability of the information systems and related processing activities.

- **War Dialling**: War dialling is a technique for systematically calling a range of telephone numbers in an attempt to identify modems, remote access devices and maintenance connections of computers that may exist on an organization’s network. Well-meaning users can inadvertently expose the organization to significant vulnerability by connecting a modem to the organization’s information systems. Once a modem or other access device has been identified, analysis and exploitation techniques are performed to assess whether this connection can be used to penetrate the organization’s information systems network.

- **Wireless network penetration testing**: The introduction of wireless networks, whether through formal, approved network configuration management or the inadvertent actions of well-meaning users, introduce additional security exposures. Sometimes referred to as “war-driving,” hackers have become proficient in identifying wireless networks simply by “driving” or walking around office buildings with their wireless network equipment. The goal of wireless network testing is to identify security gaps or flaws in the design, implementation or operation of the organization’s wireless network.
• **Social Engineering:** Often used in conjunction with blind and double blind testing, this refers to techniques using social interaction, typically with the organization’s employees, suppliers and contractors, to gather information and penetrate the organization’s systems. Such techniques could include:
  • Posing as a representative of the IT department’s help desk and asking users to divulge their user account and password information;
  • Posing as an employee and gaining physical access to restricted areas that may house sensitive information;
  • Intercepting mail, courier packages or even trash to search for sensitive information on printed materials.

Social engineering activities can test a less technical, but equally important, security component: the ability of the organization’s people to contribute to, or prevent, unauthorized access to information and information systems.

### 6.10.2 Risks associated with Penetration Testing

While management sponsors the testing activities, those activities do, in themselves, represent some level of risk. Some of the key risks include the following:

- The penetration test team may fail to identify significant vulnerabilities;
- Misunderstandings and miscommunications may result in the test objectives not being achieved;
- Testing activities may inadvertently trigger events or responses that may not have been anticipated or planned for (such as notifying law enforcement authorities);
- Sensitive security information may be disclosed, increasing the risk of the organization being vulnerable to external attacks.

Generally, penetration testing is performed by external experts, hence it is necessary to enforce non-disclosure agreement and also define content of report, since it will contain the vulnerabilities within the system.

**Table 6.2: Network Vulnerabilities and Controls**

<table>
<thead>
<tr>
<th>Target</th>
<th>Vulnerability</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precedents to attack</td>
<td>Port scan</td>
<td>Firewall</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Intrusion detection system</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Running as few services as possible</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Services that reply with only what is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>necessary</td>
</tr>
<tr>
<td>Social engineering</td>
<td>Education, user awareness</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policies and procedures</td>
<td></td>
</tr>
<tr>
<td>Network Security Controls</td>
<td>Systems in which two people must agree to perform certain security-critical functions</td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Reconnaissance</td>
<td>Firewall</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;Hardened&quot; (self-defensive) operating system and applications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intrusion detection system</td>
<td></td>
</tr>
<tr>
<td>OS and application</td>
<td>Firewall</td>
<td></td>
</tr>
<tr>
<td>fingerprinting</td>
<td>&quot;Hardened&quot; (self-defensive) applications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Programs that reply with only what is necessary</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intrusion detection system</td>
<td></td>
</tr>
<tr>
<td><strong>Authentication failures</strong></td>
<td>Impersonation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Strong, one-time authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guessing</td>
<td>Strong, one-time authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Education, user awareness</td>
<td></td>
</tr>
<tr>
<td>Eavesdropping</td>
<td>Strong, one-time authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Encrypted authentication channel</td>
<td></td>
</tr>
<tr>
<td>Spoofing</td>
<td>Strong, one-time authentication</td>
<td></td>
</tr>
<tr>
<td>Session hijacking</td>
<td>Strong, one-time authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Encrypted authentication channel</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Virtual private network</td>
<td></td>
</tr>
<tr>
<td>Man-in-the-middle attack</td>
<td>Strong, one-time authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Virtual private network</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protocol analysis</td>
<td></td>
</tr>
<tr>
<td><strong>Programming flaws</strong></td>
<td>Buffer overflow</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Programming controls</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intrusion detection system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Controlled execution environment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Personal firewall</td>
<td></td>
</tr>
<tr>
<td>Addressing errors</td>
<td>Programming controls</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intrusion detection system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Controlled execution environment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Personal firewall</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Two-way authentication</td>
<td></td>
</tr>
<tr>
<td>Parameter modification,</td>
<td>Programming controls</td>
<td></td>
</tr>
<tr>
<td>time-of-check to time-of-</td>
<td>Intrusion detection system</td>
<td></td>
</tr>
<tr>
<td>use errors</td>
<td>Controlled execution environment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Personal firewall</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Two-way authentication</td>
<td></td>
</tr>
<tr>
<td>Server-side include</td>
<td>Programming controls</td>
<td></td>
</tr>
</tbody>
</table>

37
<table>
<thead>
<tr>
<th>Module 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confidentiality</strong></td>
</tr>
<tr>
<td><strong>Confidentiality</strong></td>
</tr>
<tr>
<td>Eavesdropping</td>
</tr>
<tr>
<td>Passive wiretap</td>
</tr>
<tr>
<td>Mis-delivery</td>
</tr>
<tr>
<td>Exposure within the network</td>
</tr>
<tr>
<td>Traffic flow analysis</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Cookie</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Active wiretap</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Impersonation</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
The layers of security controls on the network are depicted in the following table.

<table>
<thead>
<tr>
<th>Falsification of message</th>
<th>Error detection code</th>
<th>Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Falsification of message</td>
<td>Firewall</td>
<td></td>
</tr>
<tr>
<td>Falsification of message</td>
<td>Encryption</td>
<td></td>
</tr>
<tr>
<td>Falsification of message</td>
<td>Strong authentication</td>
<td></td>
</tr>
<tr>
<td>Falsification of message</td>
<td>Error detection code</td>
<td></td>
</tr>
<tr>
<td>Falsification of message</td>
<td>Audit</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Noise</th>
<th>Error detection code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Noise</td>
<td>Error detection code</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web site defacement</th>
<th>Error detection code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web site defacement</td>
<td>Intrusion detection system</td>
</tr>
<tr>
<td>Web site defacement</td>
<td>Controlled execution environment</td>
</tr>
<tr>
<td>Web site defacement</td>
<td>Hardened host</td>
</tr>
<tr>
<td>Web site defacement</td>
<td>Honey pot</td>
</tr>
<tr>
<td>Web site defacement</td>
<td>Audit</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DNS attack</th>
<th>Firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS attack</td>
<td>Intrusion detection system</td>
</tr>
<tr>
<td>DNS attack</td>
<td>Strong authentication for DNS changes</td>
</tr>
<tr>
<td>DNS attack</td>
<td>Audit</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Availability</th>
<th>Protocol flaw</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>Firewall</td>
</tr>
<tr>
<td>Availability</td>
<td>Redundant architecture</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Availability</th>
<th>Protocol flaw</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmission or component failure</td>
<td>Architecture</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transmission or component failure</th>
<th>Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection flooding, e.g., echo-charge, ping of death, smurf, syn flood</td>
<td>Firewall</td>
</tr>
<tr>
<td>Connection flooding, e.g., echo-charge, ping of death, smurf, syn flood</td>
<td>Intrusion detection system</td>
</tr>
<tr>
<td>Connection flooding, e.g., echo-charge, ping of death, smurf, syn flood</td>
<td>ACL on border router</td>
</tr>
<tr>
<td>Connection flooding, e.g., echo-charge, ping of death, smurf, syn flood</td>
<td>Honey pot</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DNS attack</th>
<th>Firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS attack</td>
<td>Intrusion detection system</td>
</tr>
<tr>
<td>DNS attack</td>
<td>ACL on border router</td>
</tr>
<tr>
<td>DNS attack</td>
<td>Honey pot</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DNS attack</th>
<th>Firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS attack</td>
<td>Intrusion detection system</td>
</tr>
<tr>
<td>DNS attack</td>
<td>ACL on border router</td>
</tr>
<tr>
<td>DNS attack</td>
<td>Honey pot</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traffic redirection</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic redirection</td>
<td>Audit</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traffic redirection</th>
<th>Encryption</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Distributed denial of service</th>
<th>Firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed denial of service</td>
<td>Intrusion detection system</td>
</tr>
<tr>
<td>Distributed denial of service</td>
<td>ACL on border router</td>
</tr>
<tr>
<td>Distributed denial of service</td>
<td>Honey pot</td>
</tr>
</tbody>
</table>
Table 6.3: Layers of security controls on network

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Applicable Security/Control measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perimeter</td>
<td>Firewall</td>
</tr>
<tr>
<td></td>
<td>Network-based anti-virus</td>
</tr>
<tr>
<td></td>
<td>VPN encryption</td>
</tr>
<tr>
<td>Network</td>
<td>Intrusion detection/prevention system (IDS/IPS)</td>
</tr>
<tr>
<td></td>
<td>Vulnerability management system</td>
</tr>
<tr>
<td></td>
<td>Network access control</td>
</tr>
<tr>
<td></td>
<td>Access control /user authentication</td>
</tr>
<tr>
<td>Host</td>
<td>Host IDS and Host vulnerability assessment (VA)</td>
</tr>
<tr>
<td></td>
<td>Network access control</td>
</tr>
<tr>
<td></td>
<td>Anti-virus</td>
</tr>
<tr>
<td></td>
<td>Access control /user authentication</td>
</tr>
<tr>
<td>Application</td>
<td>Application shield</td>
</tr>
<tr>
<td></td>
<td>Access control /user authentication</td>
</tr>
<tr>
<td></td>
<td>Input validation</td>
</tr>
<tr>
<td>Data</td>
<td>Encryption</td>
</tr>
<tr>
<td></td>
<td>Access control /user authentication</td>
</tr>
</tbody>
</table>

6.11 Auditing Network Security
Auditing networked computing environments presents significant complexities. Networking enables several virtual machines to operate together using a limited set of systems resources, irrespective of the barriers of geographic location of the user and systems infrastructure. For example, a customer can now access his bank account from anywhere in the world. This means that logical paths open up enabling access through insecure networks and diverse computing infrastructures. Audit of network security requires the auditor to take special considerations into account and plan accordingly to achieve his audit objectives. The considerations while auditing network security are:

- Locating logical access paths by reviewing network diagrams
- Identifying network topologies, virtual paths spanning across LANs, WANs and the open networks such as shared networks and the Internet.
- Recognizing logical access threats, risks and exposures in the networked environment.
- Identifying and controlling over access paths used for distributed processing and distributed databases.
- Evaluating network management and change control in respect of technical components such as modems, switches, routers, firewalls, VPNs, network management and access control software, encryption, protocols, middleware controls and Internet security.
Identifying information resource owners can be quite complex since in a distributed computing environment, an application process can span several systems and networks, including those outside the organisation’s control.

Evaluating logical network security policies and practices.
Evaluating effectiveness of logical access security with respect to network security components such as:

- Firewalls and filtering routers - architecture, configuration setting as per firewall security policy, port services, anti-virus configuration, reporting and management controls
- Intrusion detection systems - architecture, configuration, interface with other security applications, reporting and management controls
- Virtual private networks - architecture, devices, protocol, encryption process integration with firewall security, change management
- Security protocols - selection of appropriate protocol, seamless security integration of protocols between devices running different protocols
- Encryption - selection of appropriate encryption methods to various application processes
- Middleware controls - middleware design and access control with respect to identification, authentication and authorisation, management of components and middleware change management.

Network event logging and monitoring

<table>
<thead>
<tr>
<th>Type of System</th>
<th>Intrusion Detection</th>
<th>Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Monitoring</td>
<td>Assessment</td>
</tr>
<tr>
<td><strong>System Control Features</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Controls</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D- Detective</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>P-Preventive</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>C- Corrective</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>S-Support</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Confidentiality**

- Unauthorized access to files and system resources
  - D: Application Based
  - P: Host Based
  - P: Target Based
  - P: Network Based
  - P: Password Assessment

- Modification to files
  - D: Application Based
  - D: Host Based
  - P: Network Based
  - P: Password Assessment

- Violation of enterprise system access policies
  - D: Application Based
  - D: Host Based
  - P: Network Based
  - P: Password Assessment
### 6.12 Summary

Networks are veins of market place. Organizations cannot imagine implementing IT without networks. Networks have added most important attribute to business performance that is efficiency. However it is not without risks. This has helps organizations in expanding their business empire and attackers in remaining unanimous. Most security breaches today are due
to availability of networks. And therefore it is most essential for organizations to protect their networks in order ensure reasonable security has been implemented. IS auditor also must focus on the network security. Although sometimes it may not be in scope, but considering the architecture auditors cannot perform any IS audit without evaluating network controls. For example if the scope of audit is application control audit, auditor have consider network since the application is accessed by users over networks and sometimes using internet.

As technology is updating its capabilities, so are attackers and they are trying to use more and more innovative methods to attack organizations. IS auditors must be aware of trends in new technology as well as current threat scenarios.

### 6.13 Questions

1. Which of the following is a method used to gather information about the communication network?
   
   A. Reconnaissance  
   B. Brute force  
   C. Eavesdropping  
   D. Wiretapping

2. Message digest helps organization in getting assurance on:

   A. Communication delivery  
   B. Data availability  
   C. Data integrity  
   D. Data confidentiality

3. While auditing organization’s network which of the following control IS auditor must verify first?

   A. Encrypted communication.  
   B. Network zoning.  
   C. Firewall configuration.  
   D. Penetration test report.

4. Cryptographic checksum is a network control that:
Module 4

A. Adds a parity bit after adding the data bits.
B. Translates data in a file into a hash value.
C. Transmits the data after encryption.
D. Translates the data into a parity checksum combination.

5. Primary function of Security operations center (SOC) is to:

A. Define baseline
B. Configure firewall
C. Monitor logs
D. Implement Antivirus

6. The intrusion detection monitoring on a host for data integrity attack by malicious software is a:

A. Technical control
B. Corrective control
C. Detective Control
D. Preventive Control

7. Which of the following is most important while performing penetration testing?

A. Maintain secrecy about testing.
B. Get consent from affected stakeholders.
C. Report to be provided to all users.
D. Perform test after office hours.

8. Most web based application attacks can be prevented by:

A. Input validation
B. Encryption
C. Penetration test
D. Access controls

9. Social engineering attacks can best be prevented by:

A. Intrusion detection system
B. Strong access controls
C. Two factor authentication  
D. Awareness training  

10. Which of the following is a type of malware that can be unintentional?  

A. Virus  
B. Logic bomb  
C. Trojan  
D. Worm  

6.14 Answers and Explanations  
1. A. Other methods are active attacks on network after getting information about networks.  

2. C. Message digest is a hash function that helps in confirming integrity of data communicated over network.  

3. B. Network segmentation or zoning is first control to implement network security. Other controls depends upon segmentation.  

4. B. Checksum is a type of hash that is used to check integrity of data after communication. It is different that parity bit that adds an extra bit for each byte and word.  

5. C. Primary function of SOC is to collect and monitor logs based on identified rules. It also defines correlation between various logs and identifies possible incidents which are communicated to respective asset owners. A is role of security manager, B and D are role of network team.  

6. C. Intrusion detection detects the possible intrusion attempt. It does not prevent or corrects it. It is a control implemented using technology.  

7. B. It is most essential to get consent from affected asset owners for before performing test, so that they can ensure that operations are not affected. Maintaining secrecy shall depend upon type of test. Report must be kept confidential and accessed only by select few. Test generally is performed when it will have least impact, but is not most important.  

8. A. Most web application attacks like SQL injection can be prevented by validating input which can reject the attackers input that can exploit vulnerability. Encryption may or may not prevent
an attack. Penetration test shall provide input on vulnerability that must be closed. Access controls may prevent some attacks.

9. D. Social engineering attack is attack on human and hence no technology can prevent it. It is best prevented by awareness training.

10. B. Logic bomb can be unintentional due to mistakes of developers going unnoticed.

6.15 References

a. Publication:

b. Websites:

1) http://compnetworking.about.com/
2) http://theirm.org/
3) http://www.cert.org/
4) http://www.isaca.org/
5) http://www.iso.org/iso/home/standards/iso31000.htm
6) http://www.webopedia.com
7) https://na.theiia.org/Pages/IIAHome.aspx
8) https://www.dataprotection.ie/
9) www.ehow.com
10) www.en.wikipedia.org
11) www.firesafetyinstitute.org
12) www.resources.infosecinstitute.com/access-control-models-and-methods
13) www.technet.microsoft.com/en-us
14) www.owasp.org