In 1-tier architecture entire processing may take place at individual terminals and a centralized machine called file server just stores the files having no role in the processing of data.

In 2-tier architecture is where processing of HTML code takes place on the client side and the web page request is processed on the server side

In 3-tier architecture, we can place our database management system or application software on a different processing zone or tier than the web server.

In a 4-tier architecture, we can place the payment processing system at the 4th tier.

**Web server** is a machine that serves up the web page requests of a client on the internet. It is a combination of hardware and software

Internet Information Server (IIS),

Middleware: Connections between e-commerce software and existing accounting system

Application program: performs a specific function such as creating invoices/bills or processing payment received from customers.

**Back Doors** are those hostile programs which, when run on a machine, install hidden services in order to give attackers remote access capabilities.

**Trojan horses** are those programs that appear harmless but actually have some malicious purpose

**Viruses and Worms** are malicious programs that can travel between computers as attachments on email or independently over a network. **Worms** spread from computer to computer, and have the capability to travel without any help or human action. **Viruses**, on the other hand, need to be activated through a human action. Another difference is that **viruses** modify existing programs on a computer unlike **worms** which can install back doors or drop viruses.

**Hackers or crackers** are those individuals who write programs or manipulate technologies to gain unauthorized access to computers and networks

**Active content** refer to programs that are embedded in web pages to cause certain action

**Active X Controls** can be used to install hidden services to the hacker.

**In Eavesdropping/ sniffing/snooping** the hacker has the ability to monitor network traffic using some kind of network monitoring software

Man in the middle attacks: attacker is able to monitor, capture and control data between sending and receiving machines

**Denial of services (DOS)** attacks: In this type of attack, the attacker gains access to the network and then send invalid data to network services or applications. These services or applications consequently become unable to perform their normal tasks or functions.

Intrusion Detection System (IDS)

A **firewall** is a combination of hardware and software that sits between the internet and internal network of an organization to protect the network from outside attack.

**Packet filter firewall ….. Circuit level firewall … Application gateway firewall**

A **proxy server** sits between an internal trusted network and the untrusted network

Virtual private network (VPN)

Remote Access Server (RAS)

Remote Access Client (RAC)

Point to Point Protocol (PPP)

Point to Point Tunneling Protocol (PPTP)

Computer Emergency Response Team **(CERT)**

Systems Administrator, Audit, Network and Security Institute **(SANS Institute)**

**Cryptography** is the technique of converting a message into unintelligible or non-understandable

**Cryptography** is a collection of mathematical techniques used to ensure confidentiality of information

The process of scrambling a message with the help of a key is **called Encryption**. The process of unscrambling a message using an appropriate key is called **decryption**

**Pretty Good Privacy (PGP)** is the name of a popular cryptographic system which is available for general public use.

**Symmetric:** In symmetric cryptography same keys are used for encryption and decryption

**Asymmetric cryptography:** pair of public and private keys is used for encryption and decryption

An **electronic signature** means any letters, numbers, symbols, images, characters in electronic form applied to an electronic document which can ensure authenticity, integrity and nonrepudiation. It uses public key cryptography

**Authenticity** means that the message is from a particular source/individual.

**Integrity** means that the message has not been altered during transmission

**Non-repudiation** means that the execution of the digital signatures cannot be denied

Digital certificates are prepared according to a generally accepted format called X.509 standard format

Hash function is a one way mathematical function applied to a message.

A message digest is a single large number typically between 128 to 256 bits in length

Hash function >> message digest >> Public Key >> encrypt the message >> digital signature >> Private Key of the sender.

The advantage of using symmetric key is that since symmetric algorithms are faster as compared to asymmetric.

Public Key Infrastructure (PKI)

Cryptographic algorithms are measured in terms of key length.

DES (Data Encryption Standard) – 56 bits

IDEA (International Data Encryption Algorithm (IDEA) – 128 bits

RC2 – (block cipher) 1-2048 bits

RC4 (stream cipher) – 1-2048 bits

Rinjdael – 128-256 bits

Following attacks have been reported on symmetric key algorithms:

**Key Search Attacks**: attempt is made by the attacker to decrypt the message with every possible key

**Cryptanalysis**: Defeated by using a combination of sophisticated mathematics and computing power

**System-based Attacks**: uses the cryptographic algorithm without actually attacking the algorithm itself

Following is the list some popular public key algorithm

1. DSS – Digital Signature Standard based on DSA (Digital Standard Algorithm) – key length is between 512-1024 bits
2. RSA
3. Elliptic Curves

**Automated Clearing House (ACH) service**. is a centralized system to which different banks are electronically connected forming a network for clearing payment requests

**SSL (Secure Socket Layer)**, which is an encryption based protocol.

**Financial Services Technology Consortium (FSTC)** is a group of U.S banks

**DigiCash**, has pioneered the use of electronic cash or e-cash. **Anonymity** of the buyer is the key feature of this system, There are three participants in it, namely, buyer, merchant and bank.

Coin = Serial#, keyversion, {Serial #}SK bank’s $1 key.

There are two main stages in this payment mechanism **– minting stage and deposit stage.**

SECURE SOCKET LAYER (SSL), developed by Netscape Communications, It operates at the TCP/IP layer of the OSI model.

When a client connects to an SSL server, the **SSL handshake begins**, which means that the two negotiate a cipher suite selecting the strongest suite the two have in common.

The greatest **advantage of SSL** is its simplicity. Since SSL is built into many browsers, no special encryption software is required either on the **client or the server side,** a drawback of SSL is that the merchant can store credit/debit card information after decryption that can be accessed by unauthorized parties from the merchant’s database.

**Secure Electronic Transaction (SET),** more sophisticated protocol, SET hides customer’s credit card information from merchants and hides order information from banks to protect privacy. This scheme is called Dual Signature.

A dual signature is created by combining two message digests and creating a new digest called **Dual Signature Message Digest (DSMD).**