UNIT 4 NETWORK SECURITY-II

Structure **Page Nos.**

4.0 INTRODUCTION

Computer security and network security can be defined as technological and managerial procedures applied to computer and network systems to ensure the availability, integrity, and confidentiality of the information managed by the computer. It implies the protection of Integrity, Availability and Confidentiality of Computer Assets and Services from associated Threats and vulnerabilities. Protection of networks and their services from unauthorised modification, destruction, or disclosure and the provision of assurance that the network will perform its critical functions correctly and that there will be any harmful side effects. The major points of weakness in a computer system are hardware, software, and data. However, other components of the computer system may also be targeted.

In this unit, we deal with advance topics of Network Security. In Section 4.2, we define digital signatures. Section 4.3 deals with management of public keys, section 4.4 presents a brief review of communication security. In section 4.5, we discuss web security. We summarise this unit in section 4.6 followed by Solutions and Answers for 'Check Your Progress'.

4.1 OBJECTIVES

The objective of this unit is to provide a practical survey of both the principles and practice of Digital Signature. After going through this unit you should be able to understand:

- digital Signature;
- public Key Infrastructure;
- management of Public Keys, and
- communication and Web Security.

4.2 DIGITAL SIGNATURES

Digital signatures are based on public key cryptography. A private key is used to create a digital signature and the public key is used to verify the digital signature. The Hash value of a message when encrypted with the private key of a person is his digital signature on that e-Document. The Digital Signature of a person therefore, varies from document to document, thus, ensuring authenticity of each word in that document. As the public key of the signer is known, anybody can verify the message and the digital signature. The *Figure 1* shows the process of creating a digital signature. The hash function is applied to the plain text which is further encrypted with the private key of a sender for creating a digital signature.

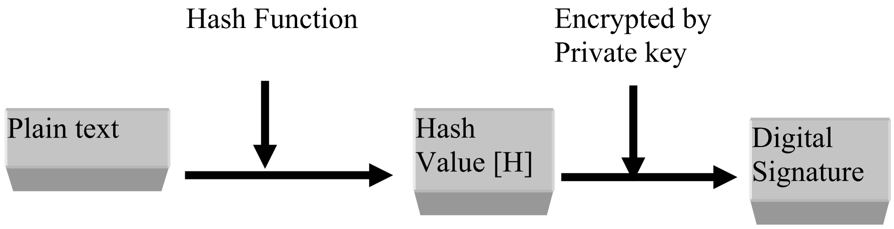


Figure 1: Digital signature

The *Figure 2* shows how one key is used for encryption and another key is used for decryption. The *Figure 3* shows that a person is having two keys in public key cryptography.

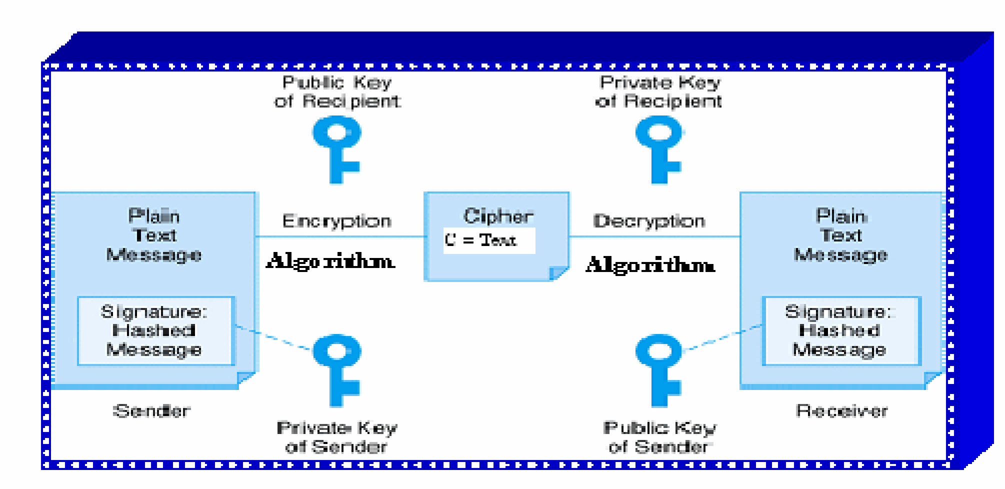


Figure 2: Encryption and signing using public key cryptography

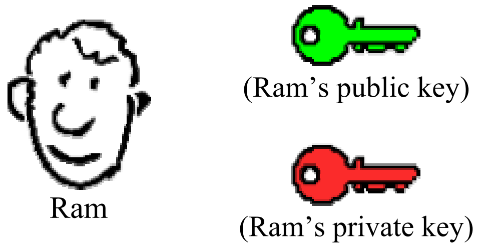


Figure 3: Explanation using an example

Ram has been given two keys. One of Ram's keys is called the Public Key, and, the other is a Private Key.

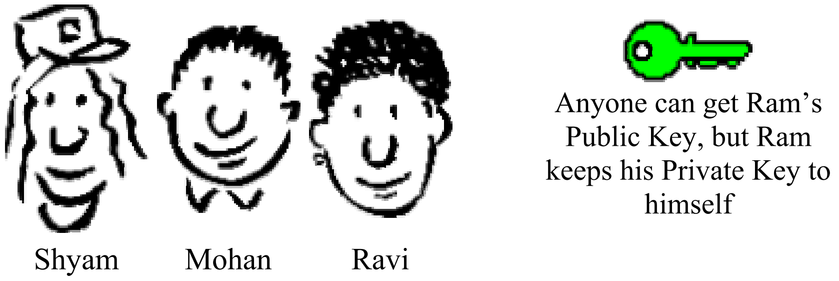

Anyone can get Ram's Public Key, but Ram keeps his Private Key to himself
Shyam
Mohan
Ravi

Figure 4:Ram's co-workers

Ram's Public key is available to anyone who needs it (*Figure 4*), but he keeps his Private Key to himself. Keys are used to encrypt information. Encrypting information means “scrambling it up”, so that only the person with the appropriate key can make it readable again. One of Ram’s two keys can encrypt the data, while the other key can decrypt that same data.

Ravi (*Figure 5*) can encrypt a message using Ram’s Public Key. Ram uses his Private Key to decrypt the message. Any of Ram’s co-workers might have access to the message Ravi encrypted, but without Ram’s Private Key, the data is worthless.

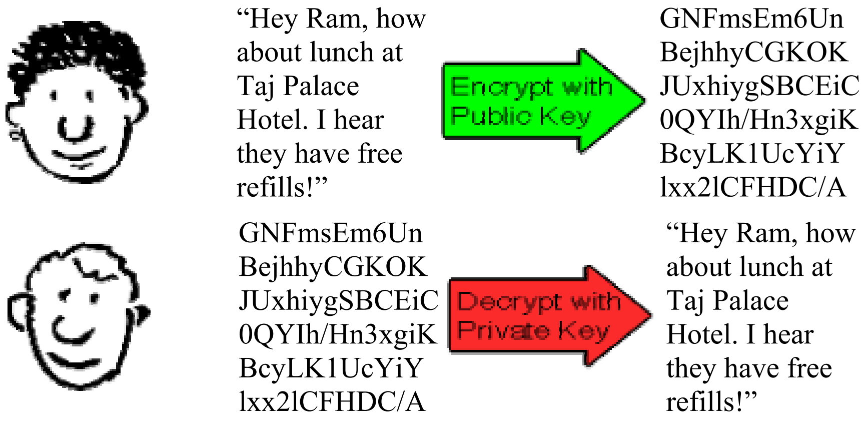
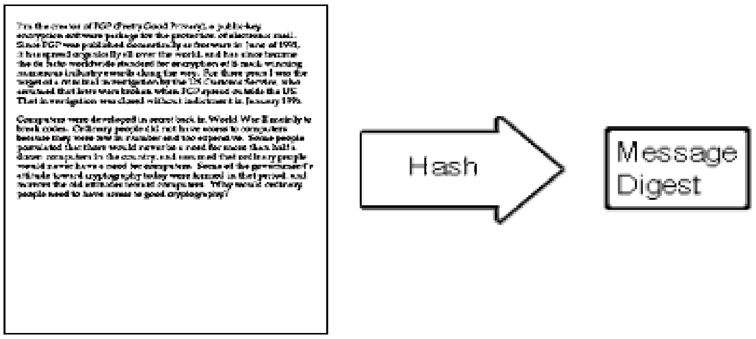

“Hey Ram, how about lunch at Taj Palace Hotel. I hear they have free refills!”
Encrypt with Public Key
GNFmsEm6Un BejhhyCGKOK JUxhiygSBCEiC 0QYIh/Hn3xgiK BcyLK1UcYiY lxx2lCFHDC/A
GNFmsEm6Un BejhhyCGKOK JUxhiygSBCEiC 0QYIh/Hn3xgiK BcyLK1UcYiY lxx2lCFHDC/A
Decrypt with Private Key
“Hey Ram, how about lunch at Taj Palace Hotel. I hear they have free refills!”

Figure 5: Encryption of a message using public key of Ram

With his private key and the right software, Ram can put digital signatures on documents and other data. A digital signature is a “stamp” Ram places on the data which is unique to Ram, and is very difficult to forge. In addition, the signature assures that any changes made to the data that has been signed will not go undetected.



I'm the creator of PGP (Pretty Good Privacy), a public-key encryption software package for the protection of electronic mail. Since PGP was published domestically as freeware in June of 1991, it has spread organically all over the world, and has since become the de facto worldwide standard for encryption of E-mail, winning numerous industry awards along the way. For three years I was the target of a criminal investigation by the US Customs Service, who assumed that laws were broken when PGP spread outside the US. That investigation was closed without indictment in January 1996.

Computers were developed in secret back in World War II mainly to break codes. Ordinary people did not have access to computers because they were few in number and too expensive. Some people postulated that there would never be a need for more than half a dozen computers in the country, and assumed that ordinary people would never have a need for computers. Some of the government's attitude toward cryptography today were formed in that period, and mirrors the old attitudes toward computers. Why would ordinary people need to have access to good cryptography?

Figure 6: Message digest

To sign a document, Ram’s software will crunch down the data into just a few lines by a process called “hashing”(*Figure 6*). These few lines are known as a message digest. (It is not possible to change a message digest back into the original data from which it was created, as Hash is a one way function).

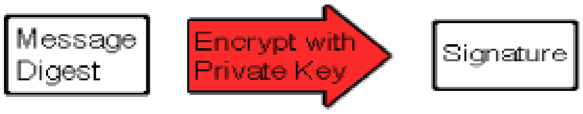


Figure 7: Encryption of a message digest using private key

Ram’s software then encrypts (*Figure 7*) the message digest with his private key. The result is the digital signature.

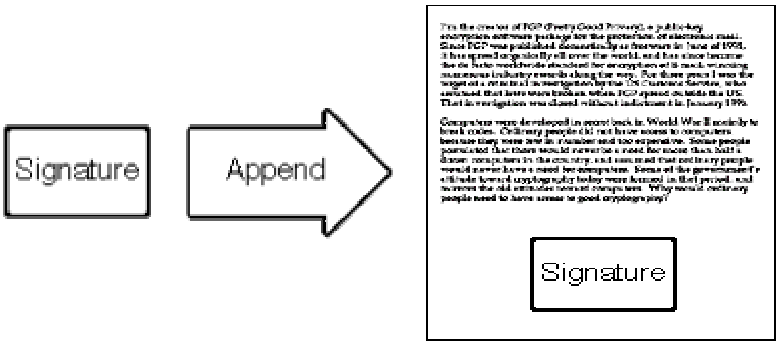


Figure 8: Append the digital signature to the document

Finally, Ram's software appends (*Figure 8*) the digital signature to the document. All the data that was hashed has been signed (*Figure 9*).

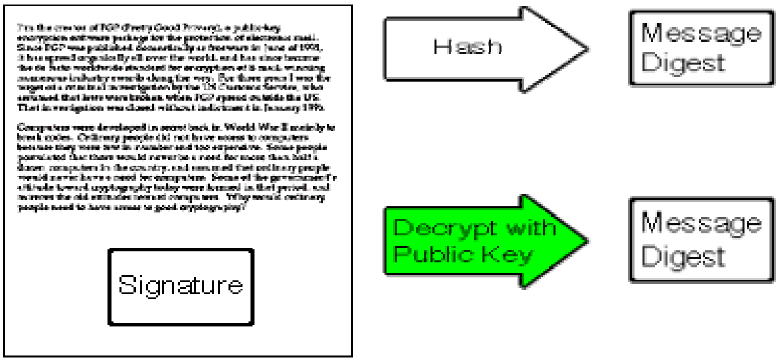


Figure 9: The decryption using public key

Ram now passes the document on to Mohan.

First, Shayam's software decrypts the signature (using Ram's public key) changing it back into a message digest. If this work, then it proves that Ram has signed the document, because only Ram has this private key. Mohan's software then hashes the document data into a message digest. If the message digest is the same as the message digest created when the signature was decrypted, then Mohan knows that the signed data has not been changed/tampered with.

Issues

Mohan (our disgruntled employee) wishes to deceive Shayam. Mohan makes sure that Shayam receives a signed message and a public key that appears to belong to Ram. Unknown to Shayam, Mohan deceitfully sends a key pair he has created using Ram's name. Short of receiving Ram's public key from him in person, how can Shayam be sure that Ram's public key is authentic?

It so happens that Ravi works at the company's certificate authority centre. Ravi can create a digital certificate for Ram by using Ram's public key as well as some information Ram (*Figure 10*).

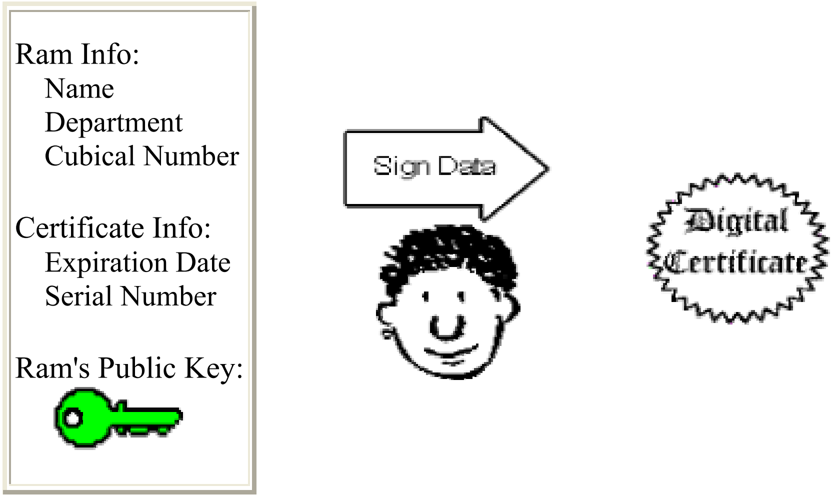


Figure 10: Creation of a digital certificate

Ram's co-workers can verify Ram's trusted certificate to make sure that his public key truly belongs to him. In fact, no one at Ram's company accepts a signature for which there does not exist a certificate generated by Ravi. This gives Ravi the power to revoke signatures if private keys are compromised, or no longer needed. There are even more widely accepted certificate authorities that certify Ravi.

If Ram sends a signed document to Shayam, to verify the signature on the document, Shayam's software first uses Ravi's (the certificate authority's) public key to check the signature on Ram's certificate. Successful de-encryption of the certificate proves that Ravi created it. After the certificate is de-encrypted, Shayam's software can check if Ram is in good standing with the certificate authority and that the certificate information concerning Ram's identity has not been altered.

Shayam's software then takes Ram's public key from the certificate and uses it to check Ram's signature. If Ram's public key de-encrypts the signature successfully, then Shayam is assured that the signature was created using Ram's private key, for Ravi has certified the matching public key. And of course, if the signature is valid, then we know that Mohan didn't try to change the signed content.

Digital Certificate

This is a certificate issued by the Certifying Authority (*Figure 11*) to the holder of the public key. The contents of a digital certificate are issued by a CA as, a data message and is always available online.

- Sr. No of the Certificate
- Applicant's name, Place and Date of Birth, Name of the Company
- Applicant's legal domicile and virtual domicile
- Validity period of the certificate and the signature
- CA's name, legal domicile and virtual domicile
- User's public key
- Information indicating how the recipient of a digitally signed document can verify the sender's public key
- CA's digital signature.

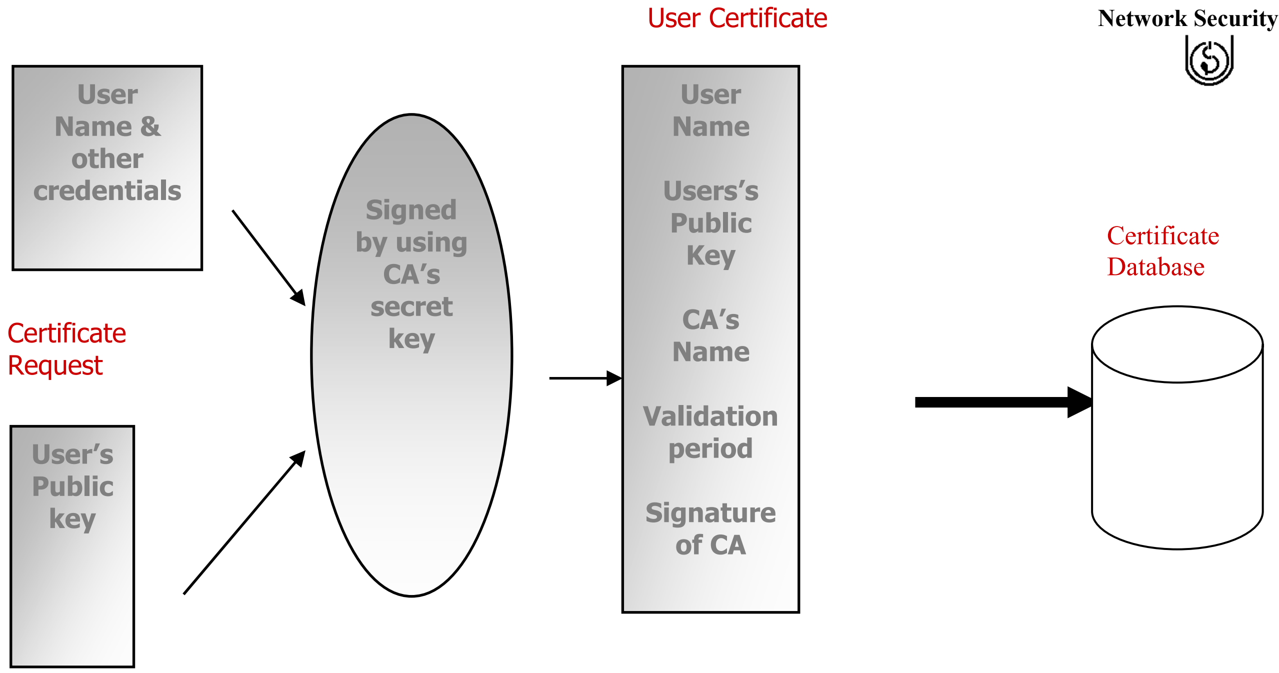


Figure 11: Issuing of a digital certificate by the certifying authority

Uses of Digital Signature

- **Contracts:** The next time you purchase a car, a home, or an insurance policy, you may never need to meet with an agent or sales representative. You may be able to review and sign all documents online, and save secure backup copies to your own disk.

- **Checks and money orders:** Buying online is now easy with a credit card, but digital checks or money orders (authenticated by secure digital signatures) may be preferable for some transactions, especially when you don't want to face a large credit card bill.

- **Letters and memos:** Businesses already transmit many letters and memos online, especially those that are only distributed internally. But when a letter or memo needs the weight of a manager's signature, it must be printed, signed, duplicated, and distributed manually or through the mail. Digital signatures will save companies the time and expense of this manual process.

- **Approvals:** Many kinds of documents are collaborative works, such as legal briefs, contracts, reports, and others. Using digital signatures, people can collaborate on documents online and approve final drafts, before/prior to releasing them for use.

☞ Check Your Progress 1

1) What does the Electronic Signatures in Global and National Commerce Act do?

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

2) What does a signature mean?

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

3) Why are handwritten signatures a drawback in some types of transactions?

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

4) What is a digital signature?

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

5) What are the benefits of using digital signatures?

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

4.3 MANAGEMENT OF PUBLIC KEYS

Public Key Infrastructure

The integration of Digital Signatures and Certificates and the other services required for E-Commerce is known as Public Key Infrastructure (PKI). These services provide integrity, access control, confidentiality, authentication, and non-repudiation for electronic transactions and communications. The PKI includes the followings: Digital certificates, Certificate authority (CA), Registration authority, policies and procedures, Certificate revocation, Non-repudiation support, Timestamping, Lightweight Directory Access Protocol (LDAP), and Security-enabled applications.

The Digital certificate and management of the certificate are the main components of PKI. The purpose of the digital certificate is to verify individual public key. This certificate is accomplished by digitally signing the individuals public key and associated information using the Private Key. A CA (Certification Authority) acts as the notary for verifying a person's identity and issuing a certificate that vouches for the public key of the individual concerned. The CA signs the certificate with its own private key. The certificate is then sent to a repository, which holds the certificates and CRLs that denote the revoked certificates.

Certificate and CRLs can be held in a repository, with well-defined responsibilities shared by both the repository and the CA. Hierarchical model followed in India is shown in *Figure 12.*

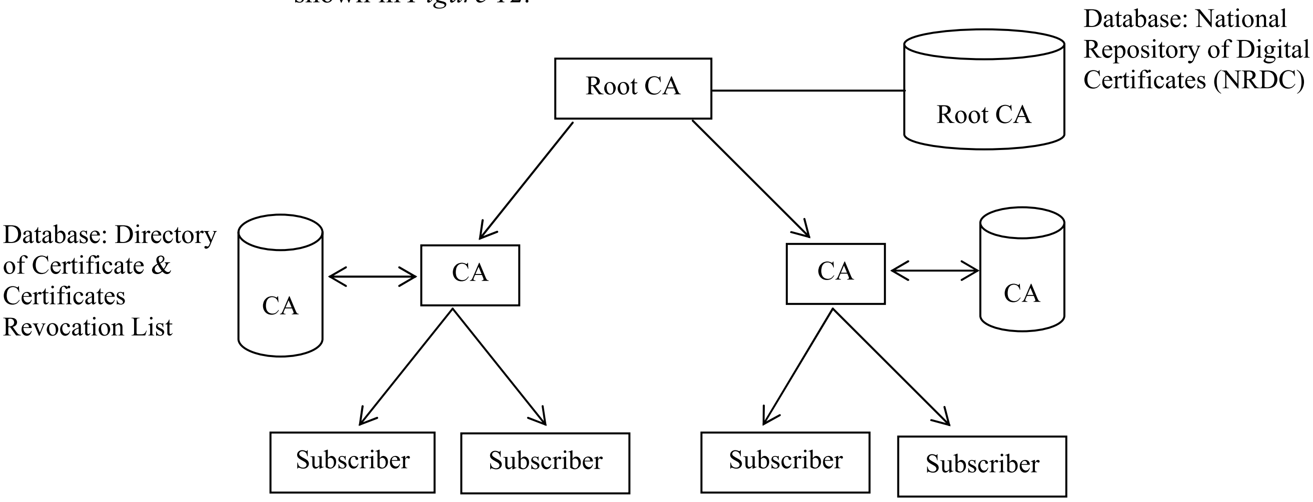

Database: National Repository of Digital Certificates (NRDC)
Root CA
Root CA
Database: Directory of Certificate & Certificates Revocation List
CA
CA
CA
CA
Subscriber
Subscriber
Subscriber
Subscriber

Figure 12: Hierarchical model being followed in India

Directories and X.500

The repository (or directory) contains entries associated with an object class. An object class can be an individual or other computer related entries. The X.509 certificate standard defines the authentification base for the X.500 directory. The X.500 directory stores information on objects in a distributed database that resides on the network server. Some of the principle definitions associated with X.500 include the following: Directory user agent (DUAs)-clients, Directory server agents (DSAs)-servers, Directory service protocol (DSP)-enables information exchanges between DSAs, Directory access protocol (DAPs)- enables information exchanges from a DUA to a DSA, and Directory information shadowing protocol (DISP)- useable information exchanges from a DUA to a DSA. DSAs accept request from anonymous source as well as authenticated requests. They share information through a chaining mechanism.

Lightweight Directory Access Protocol

The Lightweight directory access protocol (LDAP) was developed as a more efficient version of DAP and has evolved into a second version (Yeong, Y.T.Howes, and S.Killie, Lightweight Directory Access Protocol, RFC 1777,1995). LDAP servers communicate through referrals. If it finds the directory with the required entry, it sends a referral to the requesting directory. DAP v2 does not have chaining and shadowing capabilities, but additional protocol can be obtained to provide these functions.

LDAP provides a standard format for accessing certificate directories. These directories are stored on the network LDAP servers and provide public keys and corresponding X.509 certificates for the enterprise. A directory contains information such as an individual's name, address, phone number, and public key certificate. The standard under X.500 defines the protocols and information models for computer directory services that are independent of the platforms and other related entities. LDAP servers are subject to attacks that affect availability and integrity. For example, Denial of Service attacks on an LDAP server could prevent access to the CRLs and thus, permit the use of a revoked certificate. The DAP protocol in X.500 was unwieldy and led to most client implementations using LDAP. LDAP version 3 is under development; it will include extensions that provide shadowing and chaining capabilities.

X.509 Certificates

The original X.509 certyificate (CCITT, The Directory-Authentification Framework, Recommendation X.509, 1988) was developed to provide authentification foundation for the X.500 directory. Since then, a version 2,version 3, and recently, a version 4 have been developed. Version 2 of the X.509 certificates address the reuse of names, version 3 provides for certificate extensions to the core certificate fields, and version 4 provides additional extensions. These extensions can be used as needed by different users and different applications. A version of X.509 that takes into account the requirements of the internet was published by the IETF (Housley, R.W.Ford, W.Polk, and D.Solo, Internet X.509 public Key Infrastructure Certificate and CRL Profile, RFC 2459,1999).

The Consultation Committee, International Telephone and Telegraph, International Telecommunications Union (CCITT-ITU)/International Organisation for standardisation (ISO) has defined the basic format of an X.509 certificate. This structure is outlined in the *Figure 13*.

Version
Serial Number
Algorithm Identifier • Algorithm • Parameters
Issuer
Period of Validity
Subject
Subject's Public Key • Public Key • Algorithm • Parameters
Signature

Figure 13: The CCITT-ITU/ISO X.509 certificate format

If version 3 certificates are used, the optional extensions field can be used. It is before the signature field components in the certificate. Some typical extensions are the entity's name and supporting identity information, the attributes of the key, certificate policy information, and the type of subject. The digital signature serves as a tamper-evident envelope.

Some of the different types of certificates that are issued include the following:

CA certificates: Issued to CAs, these certificates contain the public keys used to verify digital signatures on CRLs and certificates.

End entity (EE) certificates: Issued to entities that are not CAs, these certificates contain the public keys that are needed by the certificate's user in order to perform key management or verify a digital signature.

Self-issued (self-signed) certificates: These certificates are issued by an entity to itself to establish points of trust and to distribute a new signing public key.

Rollover certificates: A CA issues these certificates for transition from an old public key to a new one.

Certificate Revocation Lists

The user checks the certificates revocation list (CRL) to determine whether a digital signature has been revoked. They check for the serial number of the signature. The CA signs the CRL for integrity and authentication purpose. A CRL is shown in the *Figure 14* given below for an X.509 version 2 certificates.

Version
Serial Number
Issuer
thisupdate(issue date)
nextupdate (date by which the next CRL will be issued)
revoked certificates (list of revoked certificates)
crlExtensions
SignatureValue

Figure 14: CRL format (version 2)

The CA usually generates the CRLs for its population. If the CA generates the CRLs for its entire population, the CRL is called a full CRL.

Key Management

Obviously, when dealing with encryption keys, the same precaution must be used as with physical keys to secure the areas or the combinations to the safes. The components of key management are listed as follows:

Key Distribution

As noted earlier, distributing secret keys in symmetric key encryption poses a problem. Secret keys can be distributed using asymmetric key cryptosystem. Other means of distributing secret keys include face-to-face meeting to exchange keys, sending the keys by a secure messenger, or some other secure alternate channel. Another method is to encrypt the secret key with another key, called a key encryption key, and send the encrypted key to the intended receiver. These key encryption keys can be distributed manually, but they need not be distributed often. The X9.17 Standard (ANSI X9.17 [Revised],"American National Standard for Financial Institution Key Management [Wholesale],"American Bankers Association, 1985) specifies key encryption keys as well as data keys for encrypting the plaintext messages.

Splitting the keys into different parts and sending each part by a different medium can also accomplish key distribution.

In large networks, key distribution can become a serious problem because in an N-person network, the total number of key exchanges is N(N-1)/2.Using public key cryptography or the creation and exchange of session keys that are valid only for a particular session and time are useful mechanism for managing the key distribution problem. Keys can be updated by generating a new key from an old key.

Key Revocation

A digital certificate contains a timestamp or period for which the certificate is valid. Also if the key is compromised or must be made invalid because of business-or personal-related issues, it must be revoked. The CA maintains a CRL of all invalid certificates. The user should regularly examine this list.

Key Recovery

A system must be put in place to decrypt critical data if the encryption key is lost or forgotten. One method is key escrow. In this system, the key is subdivided into different parts, each of which is encrypted and then sent to a different trusted individual in an organisation. Keys can also be escrowed onto smart cards.

Key renewal

Obviously, the longer a secret key is used without changing it, the more it is subject to compromise. The frequency with which you change the key is a direct function of the value of the data being encrypted and transmitted. Also, if the same secret key is used to encrypt valuable data over a relatively long period of time, you risk compromising a larger volume of data when the key is broken. Another important concern if the key is not changed frequently is that an attacker can intercept and change messages and then send different messages to the receiver. Key encryption keys, because they are not used as often as encryption keys, provides some protection against attacks. Typically, private keys used for digital signatures are not frequently changed and may be kept for years.

Key destruction

Keys that have been in use for long periods of time and are replaced by others should be destroyed. If the keys are compromised, older messages sent with those keys can be read.

Keys that are stored on disks or EEPROMS should be overwritten numerous times. One can also destroy the disk by shredding and burning them. However, in some cases, it is possible to recover data from disks that were put into fire. Any hardware device storing the keys, such as an EEPROM, should also be physically destroyed.

Older Keys stored by the operating system in various locations in the memory must also be searched and destroyed.

Multiple Keys

Usually an individual has more than one public/private key pair. The keys may be of different sizes for different levels of security. A larger key size may be used for digitally signing documents and smaller key size may be used for encryption. A person may also have multiple roles or responsibilities wherein s/he may want to sign messages with a different signature. One key pair may be used for business matters, another for personal use, and another for some other activity, such as being a school board member.

Distributed Vs centralised key management

A CA is a form of centralised key management. It is a central location that issues certificates and maintains CRLs. An alternative is the distributed key management, in which a “chain of trust” or “web of trust” is set up among users who know each other. Because, they know each other, they can trust that each one’s public key is valid. Some of these users may know other users and thus, verify their public key. The chain spreads outward from the original group. This arrangement results in an informal verification procedure that is based on people knowing and trusting each other.

☞ Check Your Progress 2

1) What is X.509 certificate?

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

2) List components of a X.509 Certificate and CRL certificate.

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

3) List all Certification Authorities Operating in India.

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

4.4 COMMUNICATION SECURITY

This section describes authentication mechanism to support application-level authentication and digital signatures. We will describe kerberos mechanism in the following paragraphs.

Kerberos

Kerberos is a commonly used authentication scheme on the Internet. Developed by MIT's Project Athena, Kerberos is named after the three-headed dog who, according to Greek mythology, guards the entrance of Hades (rather than the exit, for some reason!).

Kerberos (as shown in *Figure 15*) employs a client/server architecture and provides user-to-server authentication rather than host-to-host authentication. In this model, security and authentication will be based on a secret key technology where every host on the network has its own secret key. It would clearly be unmanageable if every host had to know the keys of all other hosts so, a secure, trusted host somewhere on the network, known as a Key Distribution Centre (KDC), knows the keys of all the hosts (or at least some of the hosts within a portion of the network, called a *realm*). In this way, when a new node is brought online, only the KDC and the new node need to be configured with the node's key; keys can be distributed physically or by some other secure means.

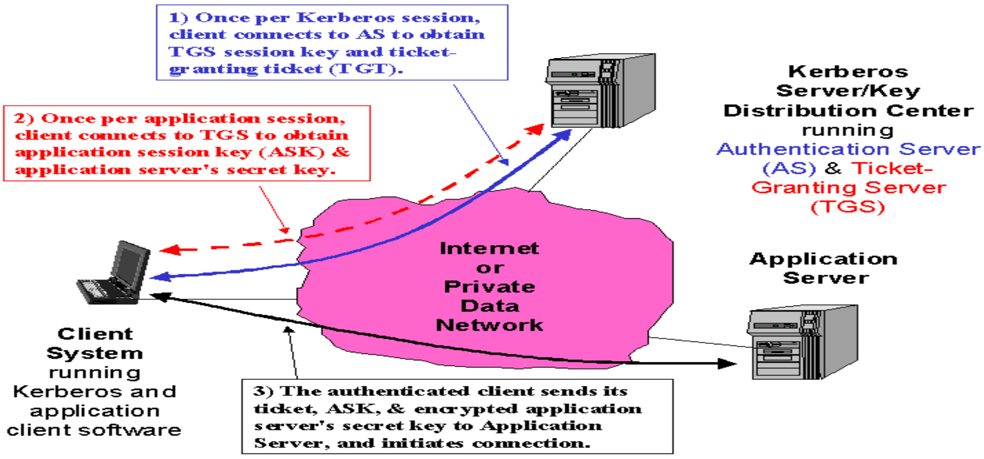

1) Once per Kerberos session, client connects to AS to obtain TGS session key and ticket-granting ticket (TGT).
2) Once per application session, client connects to TGS to obtain application session key (ASK) & application server's secret key.
Kerberos Server/Key Distribution Center running Authentication Server (AS) & Ticket-Granting Server (TGS)
Internet or Private Data Network
Application Server
Client System running Kerberos and application client software
3) The authenticated client sends its ticket, ASK, & encrypted application server's secret key to Application Server, and initiates connection.

Figure 15: Kerberos

The Kerberos Server/KDC has two main functions (*Figure*), known as the Authentication Server (AS) and Ticket-Granting Server (TGS). The steps in establishing an authenticated session between an application client and the application server are:

- The Kerberos client software establishes a connection with the Kerberos server's AS function. The AS firstly authenticates that the client is who it purports to be. The AS then provides the client with a secret key for this login session (the *TGS session key*) and a ticket-granting ticket (TGT), which gives the client permission to talk to the TGS. The ticket has a finite lifetime so that the authentication process is repeated periodically.

- The client now communicates with the TGS to obtain the Application Server's key so that it (the client) can establish a connection with the service it wants. The client supplies the TGS with the TGS session key and TGT; the TGS responds with an application session key (ASK) and an encrypted form of the Application Server's secret key; this secret key is *never* sent on the network in any other form.

- The client has now authenticated itself *and* can prove its identity to the Application Server by supplying the Kerberos ticket, application session key, and encrypted Application Server secret key. The Application Server responds with similarly encrypted information to authenticate itself to the client. At this point, the client can initiate the intended service requests (e.g., Telnet, FTP, HTTP, or e-commerce transaction session establishment).

Electronic Mail Security

Electronic mail is the most heavily used network based application. It is also the only distributed application that is widely used across all architectures and vendor platforms. With the explosively growing reliance on electronic mail, there is a concern for authentication and confidentiality of service. Two approaches, pretty good privacy (PGP) and S/MIME are widely used for this purpose.

PGP

PGP is largely the effort of a single person, **Phil Zimermann,** and provides a confidentiality and authentication service that can be used for electronic mail and file storage applications. **Zimmermann** has done the following:

- Selected the best available cryptographic functions as building blocks,
- Integrated these functions into general purpose application that is independent of operating system and processor,
- Made the package and documentation, including source code, freely available via the Internet, bulletin boards, and commercial networks, and
- Also made the Commercial versions easily available.

The actual operation of PGP consists of five services: authentication, confidentiality, compression, e-mail compatibility, and segmentation. A brief summary of PGP services is described in the Table given below:

Function	**Algorithms Used**	**Description**
Digital Signature	DSS/SHA or RSA/SHA	A hash value of the message is generated using SHA-1 algorithm. This hash value is encrypted using DSS or RSA with the sender's private key, and included with the message
Message Encryption	CAST or IDEA or 3DES with Diffie-Hellman or RSA	A message is encrypted using CAST-128 or IDEA or 3DES with a one-time session key generated by the sender. The session key is encrypted using Diffie Hellman or RSA with the recipient's public key, and attached to the message.
Compression	ZIP	A message may be compressed, for storage or transmission, using ZIP
Email-Compatibility	Radix-64-conversion	To provide transparency for e-mail applications, an encrypted message may be converted to an ASCII string using radix-64 conversion.
Segmentation	-	To accommodate maximum message size limitations, PGP performs segmentation and reassembly.

S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extension) is a security enhancement to the MIME Internet e-mail format standard, based RSA data security technology. Though both S/MIME and PGP are based on IETF standards, S/MIME is industry standard for commercial and organisational use, and PGP is a choice for personal e-mail security for many users.

MIME is an extension to the RFC 822 framework (traditional email format standard) that is intended to address some of the problems and limitations of the use of SMTP (simple mail transfer protocol) or some other mail transfer protocol and RFC 822.

Virtual Private Network (VPN)

The VPN has become the *de facto* standard for secure remote access. It provides business partners access to corporate network resources across un-trusted networks. Typically, the untrusted network will be the Internet, but VPNs offer excellent flexibility and can also be used across more traditional network mediums such as frame relay or ATM networks. VPNs guarantee the confidentiality and integrity of corporate data through the use of strong encryption and authentication techniques. VPNs have become famous because of excellent cost saving and performance improvements in comparison to more traditional remote access methods.

Types of VPN

VPNs are of two distinct categories: (1) Site to site VPNs, between two or more offices or data centres ; (2) Client to site VPNs, between a desktop client and a central office or data center.

IPSec

Most client to site VPNs are based on IPSec (short for IP Security), which is a suite of protocols developed by the IETF to support secure transmission of packets at the IP layer. Typically, an IPSec tunnel connection will be created from a Client software component to a VPN gateway (or firewall with VPN functionality). Following the initialisation of this tunnel, all packets destined for the remote corporate network will be routed through this tunnel. The tunnel provides the necessary security, by encrypting each packet (using one of a selection of algorithms) before forwarding it to the remote gateway. When packets reach the remote gateway, they are decrypted and then forwarded 'in the clear' to the final destination.

IPSec was initially devised for site to site VPN connections, so in order to add the necessary functionality to IPSec to allow effective client to site connections and management, each vendor has added vendor specific features to it's IPSec implementation. Good examples of this include Check Point hybrid mode (to allow strong user authentication without certificates) and NAT traversal techniques from the majority of vendors.

As shown in the *Figure 16*, IPSec clients work by adding extra functionality at the bottom of the IP Layer. This functionality inspects traffic, and encapsulates and encrypts traffic as necessary.

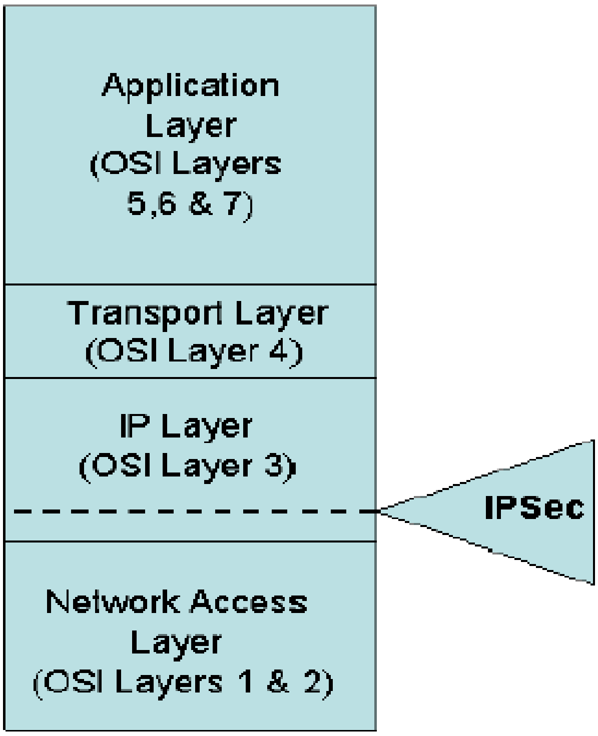

Application Layer (OSI Layers 5,6 & 7)
Transport Layer (OSI Layer 4)
IP Layer (OSI Layer 3)
IPSec
Network Access Layer (OSI Layers 1 & 2)

Figure 16: Functionality inspects traffic, and encapsulates and encrypts traffic

Secure Sockets Layer (SSL)

Netscape originated SSL. Secure Sockets layer is a protocol, which is already imbedded in most IP stacks and placed at the base of the application layer, as shown in the *Figure 17.* SSL has been traditionally and widely deployed for securing web-based applications in the form of HTTPS (or secure HTTP). Even the most novice users are normally aware of the padlock symbol shown on secure web sites, even if they are unaware of the fact that this symbol means that the site is protected by SSL.

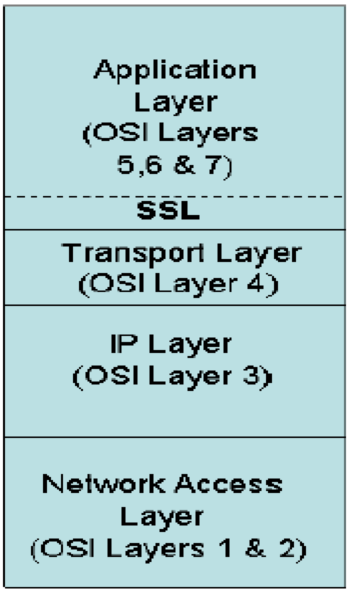

Application Layer (OSI Layers 5,6 & 7)
SSL
Transport Layer (OSI Layer 4)
IP Layer (OSI Layer 3)
Network Access Layer (OSI Layers 1 & 2)

Figure 17: Secure socket layer (SSL)

Some SSL VPNs claim to have clientless or near clientless operation. This means access to the VPN can be created from any machine with a Web browser, including machines in Internet café's and home machines. The main drivers for SSL VPN are: Cost saving; independent platform and mobility.

- **Cost saving:** Because SSL VPNs can be clientless, the cost of deploying clients is saved. For large organisations this can be a large outlay.
- **Independent Platform & mobility:** Access can be granted from many types of machine (Linux, Windows, PDAs) and from many locations.

With these benefits, SSL VPNs also has many complications and disadvantages.

Benefits of SSL

Cost saving: Because SSL VPNs can be clientless, the cost of deploying clients is saved.

Platform independence/independent platform : Access can be granted from many types of machines with different operating systems (Linux, Windows 2K/XP, Apple Mac, Palm OS, Symbian, Pocket PC).

Client type mobility: Although IPSec clients can grant access across most mediums (Leased line, DSL, Dial, GPRS) they only offer access from the corporate desktop on which the client is installed. SSL VPNs can be configured to allow access from corporate built laptops, home desktops, customer or supplier desktops or any machine in an Internet café. This extra choice allows a much wider audience (i.e., non-laptop users) to improve productivity and work from any where (at home or while travelling).

Client IP mobility: Although widespread deployment is yet to take hold, mobile IP network deployment is growing steadily. A side effect of a mobile IP network is that the client's source address can change as a client moves between cells and networks. This has the effect of breaking an IPSec VPN connection, but because SSL VPNs are not bound to the source IP address, connections can be maintained as clients move. No NAT issues - Traditionally Hide Network Address Translation (Hide NAT) has caused issues with IPSec VPNs. Vendors have generally overcome these issues by developing vendor specific NAT traversal mechanisms based on payload encapsulation in UDP packets. Although these mechanisms normally function well, they break and cause interoperability problems between vendors deployments. SSL VPNs do not suffer such issues because they are not tied to the IP layer.

Granular access control: Although IPSec VPNs also offer highly granular access control through machine and the service it provides, SSL VPNs can offer a greater degree of granularity, even as far as the URL. SSL VPNs also lend themselves to more granular access control because each resource accessed must be explicitly defined. This differs from IPSec VPN because the entire corporate network can be defined with a single statement.

Restrictive firewall rules: Organisations with a reasonable security infrastructure employs a firewall rule set with limits outbound access. SSL based VPNs communicate on the port used by Secure HTTP (TCP port 443), which is one of the few ports allowed outbound access from any machine in the corporate network in most environments. Even if the proxy cache servers are deployed, since the HTTPS traffic is encrypted, as a result, this encrypted traffic will pass un-inspected. This is not possible with IPSec based VPN.

As stated above in the *Figure 16* SSL VPNs make use of the existing SSL functionality that are already present in most IP Stacks. Because SSL fits into the stack between layers 4 and 5, each application must explicitly define its use. Based on this fact, SSL VPNs fall into 3 distinct categories: (i) Application layer proxies, (ii) Protocol redirectors, and (iii) Remote control enhancers. Commercial SSL products are a combination of the above mentioned techniques.

These techniques are discussed below:

(i) **Application layer proxies**

Application layer proxies are the simplest form of SSL VPNs because they rely on the SSL functionality used by existing applications. Because of this, application layer proxies have the least application support. Generally, they only support Email and Web-based traffic. They function by using the SSL setup in existing applications, for example, you would web browse to the gateway which will then proxy web traffic internally (using a simple method to display links to internal systems). To use the email, your administrators would configure the SSL functionality in your email client and proxy all email traffic via the gateway.

One of the advantages of application layer proxies are that they are truly clientless. They operate with nearly all operating systems and web browsers.

(ii) **Protocol redirectors**

Protocol redirectors have more flexibility than application layer proxies, but they are not truly clientless in their operation. Protocol redirectors work by downloading a mini client from the gateway, which is installed locally and redirects traffic. The redirection is depicted in *Figure 18.*

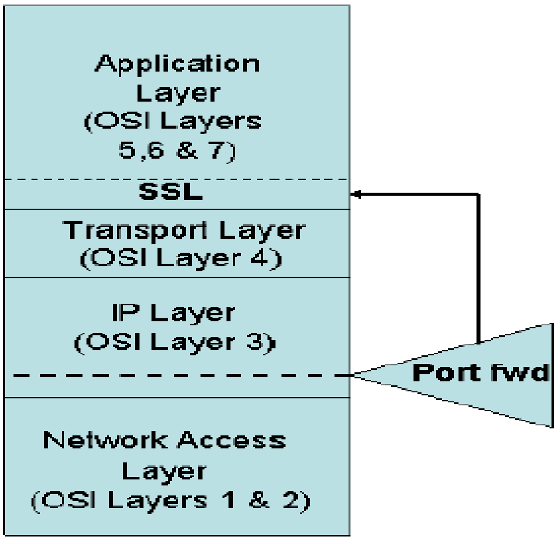


Figure18: Protocol redirector

For example, if a connection is made through an application, which does not use the SSL layer, the connection is captured at the base of the IP layer and then encapsulated within an SSL tunnel. Once the traffic reaches the SSL gateway, it is decrypted and then proxied to the original destination.

The only realistic method of capturing the traffic on the way through the IP stack is to redirect traffic based on name resolution to a local resource. For example, to connect to http://mail.yahoo.com, the port redirector is enabled, then the name mail.yahoo.com will be forced to connect to the localhost (127.0.0.1) through the use of a host file. This means that the mini client must have the ability to write changes to the hosts file, which at a hardend desktop may not always be possible. Also, in most implementations, some administrative permission is required on the local desktop to install the mini client, which is rarely possible using a machine in an Internet Café.

The main advantage of the protocol redirection system is that it can support any application that works on fixed TCP or UDP ports and in which some implementations, and applications with dynamic port applications can be supported (such as MS Outlook).

(iii) **Remote Control Enhancers**

Remote control enhancers are the most flexible form of SSL based VPN, but they also have heavy overload. They work by enhancing a remote control protocol like Windows Terminal Services or Citrix Metaframe and adding SSL VPN functionality and Web Browser support. This means any application can be added to the SSL VPN by adding the application to the remote control desktop. As a stand-alone application, this has serious limitations, because applications that reside on the local desktop cannot be used directly. This is why most remote control enhancers are partnered with other SSL VPN technologies.

On the positive side though, they can offer features like the ability to read and update a documents held centrally without ever having to download the entire document. While travelling and using VPN over low speed connections, or when connection quality is poor this could be a better option, because connections are restarted without loosing any work.

Technical Issues

Other technical considerations include: Performance; high availability; and network performance.

Performance: SSL VPNs can support large number of concurrent users with adequate performance.

High Availability: Most vendors (especially the ones with more mature products) are able to perform some form of internal High Availability and fail over mechanisms.

Network Performance: Performance over a low speed link (GSM data or GPRS) should be good to accept the mobility aspect of SSL VPNs. It has been noticed that SSL VPNs can offer some performance advantages over IPSec VPNs. Not considering the setup operations, which can be considered “one time” for a relatively short lived connection, the overhead of IPSec on a packet is between 50 and 57 octets (including the new IP header, the ESP header and the trailers), representing a 10% increase on an average packet (500 byte). In contrast to this, SSL VPNs add only 5 octets of data to each packet, just a 1% increase on the average packet. However, setup operations cannot be ignored, but these are roughly similar in size for IPSec and SSL connections. Also, because SSL VPNs work at a much higher layer, they suffer far less from, the packet fragmentation issues normally associated with IPSec VPNs. Finally, SSL has an in-built compression mechanism.

Deployment Considerations and Disadvantages of SSL VPNs.

Application Support

The main hurdle to deployment of SSL VPNs is likely to be application support. As SSL works at the boundary of layers 4 and 5, each application must support its use. Vendors add additional support through the use of protocol redirectors, but these often require some user knowledge to operate. Based on this, the first step to take when designing an SSL VPN solution is to look at the access that will be required and assess how simple this will be to provide.

Internal Network Security Failings

With IPSec VPN, a large number of organisations allocate specific IP addresses to remote clients systems using the RIDIUS Protocol. This gives the ability to file and control traffic based on the IP source, ensuring internal network security. As all sessions from an SSL VPN are normally proxied from a single address, all clients’ sessions originate from this single IP. Due to this, a network administrator is unable to allocate privileges using source IP addresses. In reality, this level of control can be handled on the SSL VPN gateway, but if a network is already configured to some IP source based security, the overhead of altering it, can be very high.

Audit and Activity Awareness

Any security appliance, hardware or software system should include a good level of auditing. With SSL VPN this functionality is seen as the key, because of the relatively simple systems needed to abuse an SSL VPN by a remote hacker (i.e., A web browser), should logon credentials become compromised. Further to this, some form of real time alerting of unusual actions (such as trying to copy an entire disk over the VPN) must be included. Some of this functionality is seen by vendors, as fewer keys and, is still evolving.

Client Security

As SSL VPN offers a much greater choice of client platform with 'clientless' or 'near clientless' operation, the security of any client connecting to the network must be scrutinised. For example, in no way would any organisation consider a PC in an Internet café to be as trusted as a corporate issued laptop. Due to this, vendors have developed several mechanisms to boost the trust associated with an un-trusted client connection. Some of these are outlined below:

Client Integrity Scanning

When a client connects to the VPN a small java applet is downloaded to the client machine, which searches for good or bad files, process or ports listening. For example, it can check for a running AV program with current definitions, the presence of a personal firewall with a standard rule set or the presence of any known Trojans. The disadvantage of this mechanism is it may place limitations on the types of clients that can connect, but more importantly, it is only a onetime snapshot of a system. Also with an understanding or the rule set, it seems feasible that these checks may be fooled.

Sandbox

A sandbox is used to store any files downloaded from a corporate network over the SSL VPN. Once the VPN session is terminated, the contents of the sandbox are securely deleted. This avoids issues of email attachments and corporate data being accidentally left on un-trusted machines. Sandboxes can also be used to ensure Citrix Metaframe or other interactive session data is wiped from a machine at logoff.

Secure logoff and credential wiping: This ensures that when users logoff the system, all logon credentials are wiped from the client machine. Of course, with enterprise strength VPN solution, a strong authentication mechanism should also be used to protect credentials further.

Timeouts and Re-authentication

To avoid systems being left connected to the network by users, sessions can be terminated after periods of inactivity. Also, to ensure that the correct user is still using the connection, periodic authentication during a session can be implemented on client systems.

Virus, Malicious Code and Worm Activity

As the client is nearly un-trusted, most SSL VPNs can also filter traffic at the application level (especially if an application level proxy is used, rather than a protocol redirector), blocking worms and viruses at the gateway.

SSL VPNs used for remote access, no doubt, have significant advantages over the IPSec alternatives. But the advantages they offer also add complexity, which must be weighed against the advantages. Before considering an SSL VPN deployment you should consider: security risks involved; added mobility and flexibility; protocol support required.

4.5 WEB SECURITY

With the transformation of the Internet from a network used primarily by universities and research laboratories to a world-wide communications medium, attacks on the World Wide Web and Internet can be have very serious consequences. In today's environment virtually all businesses, government agencies, and many individuals now have their own web sites. But Internet and Web are extremely vulnerable to compromises of various sorts. As a result demand for secure web services grows. Thus, there is a need for protecting nodes on the Internet and for providing for the confidentiality, integrity, and availability of information utilising these networks.

Web Security Considerations

WWW is fundamentally a client/server application running over the Internet and TCP/IP intranet. This presents new challenge:

- The web is vulnerable to attacks on the Web server over the Internet.
- Reputation can be damaged and money can be lost if the Web servers are subverted, as it serves as a highly visible outlet for corporate and product information.
- The history of the web show that even upgraded, properly installed systems are vulnerable to a variety of security attacks.

SSL/TLS

The Secure Sockets Layer (SSL) protocol was developed by Netscap in 1994 to protect the confidentiality of information transmitted between two applications, to verify the integrality of communication and to provide authentication means in both directions. SSL implements these functions using public and private key encryption and a message authentication code (MAC).

Microsoft has developed a newer version of SSL, Transport Layer security (TLS). As with SSL,TLS includes confidentiality, integrity and authentication above the transport layer and is application independent. Because SSL and TLS ride on the transport layer protocol, they are independent of the application. Thus, SSL and TLS can be used with application such as telnet, FTP, HTTP and email protocol.

Both SSL and TLS use certificates for public key verification that are based on the X.509 standard.

SSL 3.0

The design goals of SSL 3.0 were to provide:

1) **Cryptographic Security:** Protection of the confidentiality of transmitted messages.

2) **Interoperability:** Application should be able to be developed using SSL 3.0 by groups of individuals without knowledge of each other's code.

3) **Extensibility:** The ability to incorporate different encryption algorithm into SSL 3.0 without major changes to SSL 3.0.

4) **Relative Efficiency:** Efficient utilisation of computing and network resources.

Session keys generated during SSL private key cryptography transaction are either 40-bits or 128-bits in length. Newer browsers support 128-bit encryption.
The SSL protocol comprises two layers, the SSL Record Protocol and the SSL Handshake Protocol. The SSL Record Protocol is layered above a transport protocol, such as TCP. This record protocol is used for encapsulation of higher-level-protocols, such as the SSL Handshake protocol. The latter protocol is used for client/server mutual authentication, negotiation of a cryptographic algorithm, and exchange of cryptographic keys.

Thus, through these mechanisms, SSL provides:

a) Mutual authentication using public key cryptography based on algorithms, such as, the Digital Signature Standard (DSS) and RSA.

b) Encryption of messages using private key cryptography based on algorithm, such as, IDEA, 3DES, and RC4.

c) Integrity verification of the message using a keyed message authentication code (MAC) based on hash functions, such as, MD% and SHA.

TLS 1.0

Similar to SSL, the TLS protocol is comprised of the TLS Record and Handshake Protocols. The TLS Record Protocol is layered on top of a transport protocol such as TCP and provides privacy and reliability to the communications. The privacy is implemented by encryption using symmetric key cryptography (DES or RC4). A new secret key is generated for each connections; but, the Record Protocol can be used without encryption. Integrity is provided through the use of a MAC (Message Authentication Code) using hash algorithms such as SHA or MD5.

The TLS Record Protocol is also used to encapsulate a higher-level protocol such as the TLS Handshake Protocol. The server and client use this Handshake Protocol to authenticate each other. The authentication can be accomplished using asymmetric key cryptography (RSA or DSS). The Handshake Protocol also sets up the encryption algorithm and cryptographic keys to enable the application protocol to transmit and receive information.

Since TLS is based on SSL, they have similar functionality and goals; however, SSL and TLS have enough differences that they cannot interoperate. In order to address this situation, TLS through built-in mechanism becomes compatible with SSL 3.0.

S-HTTP

Secure HTTP (S-HHTP) is a communication protocol for providing secure messaging over HTTP. S-HTTP provides equal and symmetric capabilities to both client and server, but when an entity that is S-HTTP enabled communicates with another entity that is not S-HTTP capable, the secure features will not work. S-HTTP implements secure, end-to-end transactions. S-HTTP supports a symmetric key encryption only mode, and therefore, does not require public key encryption for key exchanges. It is flexible, but permits the clients and servers to use different forms of transactions related to the signing of messages, encryption of messages, algorithms used, and types of certificates. S-HTTP protocol supports the following:

- Option negotiations for defining the type of transactions desired,
- A variety of key management mechanisms,
- Various trust models,
- Multiple cryptographic algorithms,
- Multiple operation modes, and
- Different encapsulation formats.

Instant Messaging

Instant messaging supports the real time exchange of messages between two parties using the Internet. To use this service, the user has to have instant messaging client software on his or her computer system. The client software then communicates with an instant messaging server. Some popular messaging utilities are the freeware ICQ (for "I seek you" at www. Icq.com), AIM (America Online's Instant Messenger), Microsoft's instant messaging utility in MSN Explorer, and Yahoo Instant Messenger.

One problem with instant messaging is lack of interoperability. A person with an instant messaging utility from one source or vendor may not be able to communicate with a person using a different instant messaging package. To solve this problem, the Internet Engineering Task force (IETF) has developed a standard protocol for instant messaging- the Instant Messaging Presence Protocol.

IM Vulnerabilities

Messages sent through the instant messaging protocol are not inherently secure and safe. The instant messaging server is vulnerable because it contains both the messages and the connection information of the user. Thus, instant messaging servers should be secure servers located in protected and limited access areas. In addition to that, some of the security features provided by some instant messaging software utilities include:

- encryption, integrity, and authentication services using SSL,
- authentication against propriety databases, domains, or LDAP,
- secure transfer of files,
- ability to use any TCP port,
- web-based tools for administration of the instant messaging network on the instant messaging server, including tools for user account administration, logging of critical data, and analysis of log information.

Naming Conventions

New Technology File Systems (NTFS) has the capability to generate names in the DOS 8.3 naming convention to service 16-bit application that access files that do not conform to DOS 8.3 naming. Windows 2000, Windows NT, and Windows NT Workstation support the NTFS file system. Windows 95/98 support, the earlier FAT file system along with the FAT 32, new version. The NTFS enhancement over FAT/FAT32 includes optimisation of available disk space, fault tolerance, and improved security features.

Web servers that respond to requests for files in their DOS 83 fields names are vulnerable to attacks that can cause the server to reveal source code. A fix to this problem is, to disable DOS 8.3 file name creation on the NTFS server, but this may result in difficulties in using 16-bit applications.

☞ Check Your Progress 3

1) Which choice below most accurately describes SSL?

   (i) It's a widely used standard of securing email at the Application level.

   (ii) It gives a user remote access to a command prompt across a secure, encrypted session.

   (iii) It uses two protocols, the Authentication header and the Encapsulating Security Payload.

(iv) It allows an application to have authenticated, encrypted communication across a network.

2) List differences between SSL and TLS.

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

3) What is S-HTTP?

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

4) What are instant messaging and its vulnerabilities?

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

4.6 SUMMARY

Computer and Network security relates to technological and Managerial procedures applied to a computer, computer system, computer network to ensure the availability, integrity and confidentiality of data. In this unit covered various aspects of digital signatures, management of public keys, public key infrastructures in India, Communication and web security etc.

4.7 SOLUTIONS/ANSWERS

Check Your Progress 1

1) It forms the basis for e-commerce. And it is legally equated at par with the Hand signature or paper signature (On line tracking, secure communication, E-commerce, on-line shopping etc.

2) It means the any *Figure*, combination words etc. that belongs to owner and owner only. And no-one else can imitate easily.

3) It is possible to forge handwriter with little practice and for verification you need a handwriting expert. So all such transaction where two parties are staying for apart the authenticity, integrating etc. these signature are questionable.

4) It is electronic equivalent of paper signature. It is actually hash of the message encrypted by the private key of the owner.

5) 1. It is simple to use.
2. It is content dependent.
3. It is very easy to verify without having any need for any expert.
4. You can verify Authenticity, integrity, non-repudiation.

Check Your Progress 2

1) It is Digital signature certificates format standard. And digital signature certificates are published using this format.

2) X.509 Certificate Component are: Version, Serial Number, Algorithm, Identifier, Issuver, period of validity, subject, subject's publicity, signature (see *Figure x 509 certificate format)*.

   CRL Certificate Components are: Version, Serial No. Issuer, this update, next update revoked certificates, CRL extension, signature value (see *Figure CRL format)*.

3) The Following are the functions
   1. NIC (National Informatics Centre)
   2. TCS
   3. Safescrypt
   4. GNFC
   5. Customer & Central Excise
   6. MTNL
   7. IPRBT

Check Your Progress 3

1) (i)

2) Please see SSL 3.0 & TLS 1.0

3) It is secure HTTP & used for providing secure messaging over HTTP (Please see S-HTTP).

4) It is real time exchange of messages between the two parties, its vulnerabilities are lack of inter possibility and are not inter secure & safe. It is not safe as it containing both the messages and the connection information of the user.

4.8 FURTHER READINGS

1) *Network Security Essential - Application and standard*, William Stallings, Pearson Education, New Delhi.

2) *Computer Networks,* A.S. Tanenbaum, 4th Edition, Practice Hall of India, New Delhi, 2002.