BACHELOR OF COMPUTER APPLICATIONS

SEMESTER 4

DCA2201

COMPUTER NETWORKING

Unit 14

Network Security

Table of Contents

1. INTRODUCTION

In the previous unit, we have discussed multimedia networking. Multimedia data includes audio, video and images constitutes the majority of traffic on the internet by many measures. In this unit, we will discuss network security. Nowadays, millions of people are using the internet for banking, shopping and other similar purposes and network security is a major concern. In this unit, we will discuss network security from various angles. Most security issues are created intentionally by malicious users who are attempting to get some benefit or trying to harm someone.

We begin this unit with a discussion on communication security, which deals with the transmission of data from source to destination without modification. In the next section, we will discuss e-mail security which covers two techniques for e-mail security, PGP and S/MIME. In the last section, we will explore web security. In web security, we will discuss secure naming, secure socket layer and mobile code security.

1.1 Objectives:

After studying this unit, you should be able to:

- *Describe IPSecurity*
- *Explain firewalls*
- *Describe virtual private networks*
- *Describe wireless security*
- *Explain PGP*
- *Describe S/MIME*
- *Describe web security*

2. COMMUNICATION SECURITY

Communication security deals with the transfer of data from source to destination without any modification. Main aim of security is to prevent unwanted modification by malicious users. We will discuss different techniques for communication security and its implementation in the following sections.

2.1 IP Security (IPSec)

Internet Protocol Security (IPSec) is a protocol suite for securing communications using internet protocol (IP) by authenticating and encrypting each IP packet of a communication. The complete IPSec design is a framework for multiple services such as secrecy, data integrity and protection from replay attacks. Even though IPSec is in the IP layer, it is connection oriented.

IPSec has two main parts. The first part describes two new headers. These headers can be added to packets to carry the security identifier, integrity control data, and other information. The second part, which is known as Internet Security Association and Key Management Protocol (ISAKMP) deals with establishing keys. The main protocol for carrying out the work is IKE (Internet Key Exchange).

IPSec can be used in two modes. They are *transport mode* and *tunnel mode.* In transport mode, the IPsec header is inserted just after the IP header. The *Protocol* field in the IP header is changed to indicate that an IPsec header follows the normal IP header. The IPsec header contains security information, a new sequence number, and an integrity check of the payload.

In tunnel mode, the entire IP packet and header is encapsulated in the body of a new IP packet with a completely new IP header. Tunnel mode is useful when the tunnel ends at a location other than the final destination. For example, in some cases, the end of the tunnel is a security gateway machine such as a company firewall. In this case, this security gateway encapsulates and decapsulates packets as they pass through it. By terminating the tunnel at this secured machine, the machines on the company LAN do not have to be aware of IPsec. Only the security gateway has information about it. Tunnel mode is useful when a group of TCP connections is combined and handled as one encrypted stream because it prevents an intruder from seeing who is sending how many packets to whom. Tunnel mode also provides a way to traffic analysis (analysing the flow of patterns). The disadvantage of tunnel mode is that it adds an extra IP header which increases the packet size. In transport mode, packet size is not affected.

Following are some of the important features of COMSEC:

- Transmission security, physical security, cryptographic security, emission securities are the basic elements of COMSEC.
- It provides security of the messages by encryption.
- Various cipher algorithms can encrypt or decrypt the messages.

Elements of COMSEC

- Cryptographic security: The component of communications security that results from the provision of technically sound cryptosystems and their proper use. This includes ensuring message confidentiality and authenticity.
- Emission security (EMSEC): The protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from communications systems and cryptographic equipment intercepts and the interception and analysis of compromising emanations from cryptographic—equipment, information systems, and telecommunications systems.[1]
- Transmission security (TRANSEC): The component of communications security that results from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis (e.g. frequency hopping and spread spectrum).
- Physical security: The component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons.

Technical threats to communication security

- Authentication
- Confidentiality
- Integrity
- Availability

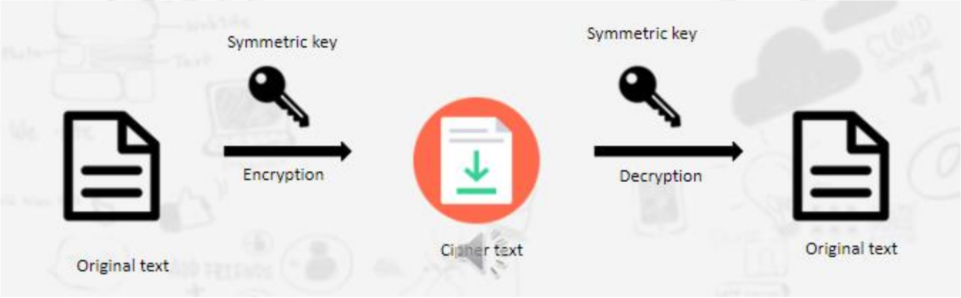
A scrambler is a device that transposes or inverts signals or otherwise encodes a message at the sender's side to make the message unintelligible at a receiver not equipped with an appropriately set descrambling device. Whereas encryption usually refers to operations carried out in the digital domain, scrambling usually refers to operations carried out in the analog domain.

Analog Scrambling

- Time element scrambling
- Digital ciphering
- Frequency Scrambling
- Digital stream ciphering
- Block ciphering

Symmetric Cipher

- Ciphers or algorithms can be either symmetric or asymmetric. Symmetric ones use the same key (called a secret key or private key) for transforming the original message, called plaintext, into ciphertext and vice versa.
- Symmetric ciphers are generally faster than their asymmetric counterparts, which use a closely-held private key as well as a public key shared between the two parties (hence public-key cryptography, or PKC).
- Examples of symmetric ciphers are Advanced Encryption Standard (AES), Data Encryption Standard (DES), Blowfish, and International Data Encryption Algorithm (IDEA).



- The use of a symmetric cipher presents the familiar challenge of how to share the secret key between the parties securely, as an unauthorized party to the conversation may intercept it and eavesdrop on future conversations.
- As a solution, an asymmetric cipher is typically used for the key exchange. Examples of widely-used key-exchange asymmetric ciphers include the Diffie–Hellman key exchange protocol, the Digital Signature Standard (DSS, which incorporates the Digital Signature Algorithm or DSA), various elliptic curve techniques, and the RSA encryption algorithm.

Encryption
Encryption key
Public key
Decryption key
Private key
Decryption

2.2 Firewalls

Firewall is a network security system to prevent unauthorized access by controlling theincoming and outgoing traffic. Firewall acts as a packet filter. It checks all the incoming and outgoing packets. Packets meeting some criterion described in rules created by the network administrator are forwarded normally. Those that fail the test are dropped. The filtering criterion is typically given as rules or tables that list sources and destinations that are acceptable, sources and destinations that are blocked, and default rules about what to do with packets coming from or going to other machines. Figure 14.1 shows an example firewall system.

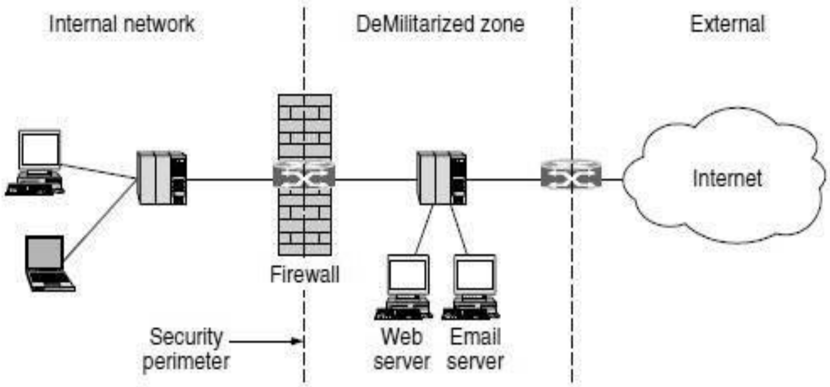


Fig 14.1: A firewall protecting an internal network

Firewalls apply rules independently to each packet. There are different firewalls based on where the communication is taking place. ***Stateful firewalls*** map packets to connections and use TCP/IP header fields to keep track of connections. This allows for rules that allow an external web server to send packets to an internal host, only if the internal host first establishes a connection with the external web server. This type of rule is not possible with stateless designs. In stateless, it must either pass or drop all packets from the external Web server.

Next generation firewall or another level of advancement from stateful processing is for the firewall to implement ***application-level gateways***. This processing involves the firewall inspecting inside packets, beyond even the TCP header, to see what the application is doing. With this ability, it is possible to distinguish HTTP traffic used for web browsing from HTTP traffic used for peer-to-peer file sharing.

Even if the firewall is well configured, many security problems still exist. For example, if a firewall is configured to allow in packets from only specific networks, an intruder outside the firewall can put in false source addresses to bypass this check. If an insider wants to transfer secret documents, he can encrypt them or even photograph them and ship the photos as JPEG files, which bypasses any email filters. Another type of attack in which the attacker is trying to shut down the target rather than steal data are called DoS (*Denial of Service*) attacks. Generally, these request packets have false source addresses so the intruder cannot be traced easily. DoS attacks against major web sites are common on the Internet.

2.3 Virtual Private Networks

Many companies have offices located over many cities. Earlier, before public data networks, such companies leased lines from telephone companies for all of their locations. This type of network which is built up from company computers and leased telephone lines is called a **private network.** Leasing a dedicated T1 line between two locations costs more, and T3 lines are many times more expensive. In such a situation, when public data networks and internet appeared, many companies wanted to move their data to public network, without compromising the security of private network. This led to the invention of **VPNs (Virtual Private Networks),** which are overlay networks on top of public networks but with most of the properties of private networks.

One popular approach is to build VPNs directly over the Internet. A common design is to fit each office with a firewall and create tunnels through the Internet between all pairs of offices, as shown in figure 14.2 (a). Another advantage of using internet for connectivity is that the tunnels can be set up on demand. So flexibility is much more compared to leased lines. From the perspective of the computers on the VPN as shown in figure 14.2 (a), the topology looks just like the private network case as shown in figure 14.2 (b).

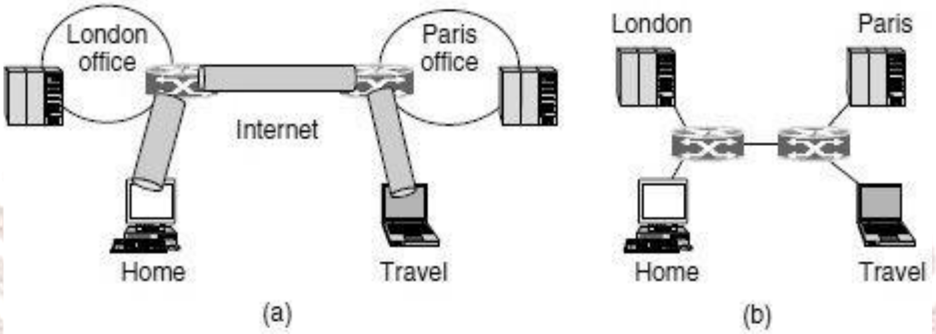


Fig 14.2: (a) A virtual private network. (b) Topology as seen from the inside

When the system is brought up, each pair of firewalls has to negotiate the parameters of its Security Association (SA), including the services, modes, algorithms, and keys. If IPsec is used for the tunnelling, it is possible to aggregate all traffic between any two pairs of offices into a single authenticated, encrypted SA, thus providing integrity control, secrecy, and even considerable resistance to traffic analysis. In many firewalls, VPN capabilities are built in.

After establishing the security association, traffic begins flowing. When considering a router's perspective, the packet traveling along the VPN tunnel is just an ordinary packet. The difference is that it includes an IPsec header after the IP header. But since these extra headers have no effect on the forwarding process, the routers do not care about this extra header. Main advantage of a VPN is that it is completely transparent to all user software. The firewalls set up and manage the security association. The only person who is even aware of this setup is the system administrator who has to configure and manage the security gateways.

2.4 Wireless Security

Wireless security deals with the prevention of unauthorized access to the devices using wireless networks. Part of the IEEE802.11 standard, which is called ***802.11i,*** dictates a data link level security protocol for preventing a wireless node from reading or interfering with messages sent between another pair of wireless nodes. It also has the trade name ***WPA2 (WiFi Protected Access 2).*** The first generation of 802.11 security protocol is known as ***WEP (Wired Equivalent Privacy)***. WiFi Protected Access is a replacement for WEP. The current WPA standard is WPA2. WPA2 uses an encryption device that encrypts the network with a 256-bit key. This longer key length improves security.

Nowadays, the use of WEP is strongly discouraged because there are many softwares to crack WEP passwords. WPA (802.11i) provides real security if it is properly set up and used. There are two common scenarios in which WPA2 is used. The first is a corporate setting, in which a company has a separate authentication server that has a username and password database that can be used to determine if a wireless client is allowed to access the network. In this case, clients use standard protocols to authenticate themselves to the network. Two main standards are 802.1X and EAP (Extensible Authentication Protocol). 802.1X, by which the access point allows the client to continue a dialogue with the authentication server and observes the result. EAP tells how the client and authentication server interact.

The second scenario is in a home setting in which there is no authentication server. A single shared password is used by clients to access the wireless network. This setup is less complex and less secured as well.

Bluetooth Security

When compared to 802.11, Bluetooth has a shorter range. Bluetooth version 2.1 and later versions have four security modes. This modes includes a no security to full data encryption and integrity control. Bluetooth provides security in multiple layers. Before version 2.1, two devices were assumed to share a secret key set up in advance. These shared keys are known as passkeys. These keys are easily predictable and less secure.

Another security issue with Bluetooth is that it authenticates only devices, not users, so theft of a Bluetooth device may give the thief access to the user’s financial and other accounts. Bluetooth implements security in the upper layers, so even in the case of theft or the break of link level security, some security will still remain, especially for applications that require a PIN code to be entered manually from some kind of keyboard to complete the transaction.

SELF-ASSESSMENT QUESTIONS – 1

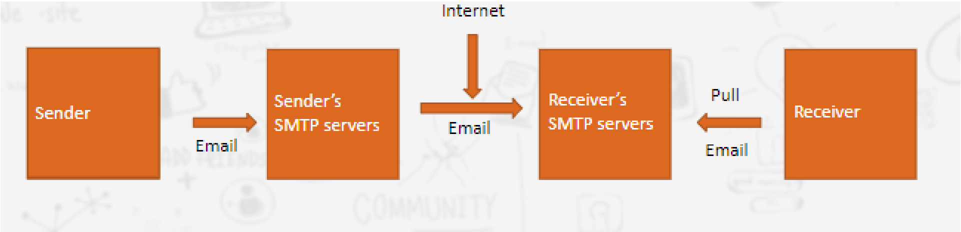
1. Internet Protocol Security (IPSec) is a protocol suite for securing communications using ____________________.
2. IPSec can be used in two modes. They are____________________ and ____.
3. Firewall is a network security system to prevent unauthorized access by controlling the incoming and outgoing traffic. State true or false.
   a) True (b) False
4. Firewalls map packets to connections and use TCP/IP header fields to keep track of connections.
5. Overlay networks on top of public networks but with most of the properties of private networks is called _________________.
6. The first generation of 802.11 security protocol is known as_______________.

3. E-MAIL SECURITY

When a sender sends an e-mail to a receiver, this e-mail is transmitted through different machines in the network before reaching the final destination. Any of these intermediaries can read and record the messages. In order to avoid such a situation, we generally apply cryptographic principles to email to produce secure email. In the following sections, we will discuss widely used secure email system, PGP and S/MIME.

Email Security Requirements

- Non-repudiation
- Integrity
- Authentication
- Confidentiality



3.1 PGP – Pretty Good Privacy

Phil Zimmermann created PGP in 1991. PGP is a complete email security package that provides privacy, authentication, digital signatures, and compression. The complete package, including all the source code, is distributed free on the Internet. Due to its quality, zero cost, and easy availability on UNIX, Linux, Windows, and Mac OS platforms, it is widely used today. PGP encrypts data by using a block cipher called ***IDEA (International Data Encryption Algorithm),*** which uses 128-bit keys.

PGP supports text compression, secrecy, and digital signatures and also provides extensive key management facilities. It is like a pre-processor that takes plaintext as input and produces signed ciphertext in base64 as output. Let's see how PGP works. Consider the example given in figure 14.3. In the example, Alice wants to send a signed plaintext message, P, to Bob in a secure way. Both Alice and Bob have private (*DX*) and public (*EX*) RSA keys. Also assume that each one knows the other's public key. Alice starts out by invoking the PGP program on her computer. PGP first hashes her message, *P*, using the hash algorithm and then encrypts the resulting hash using her private RSA key, *DA*. When Bob receives the message, he can decrypt the hash with Alice's public key and verify that the hash is correct.

The encrypted hash and the original message are now concatenated into a single message, *P1*, and compressed using the ZIP program. Output of this step is P1.Z.

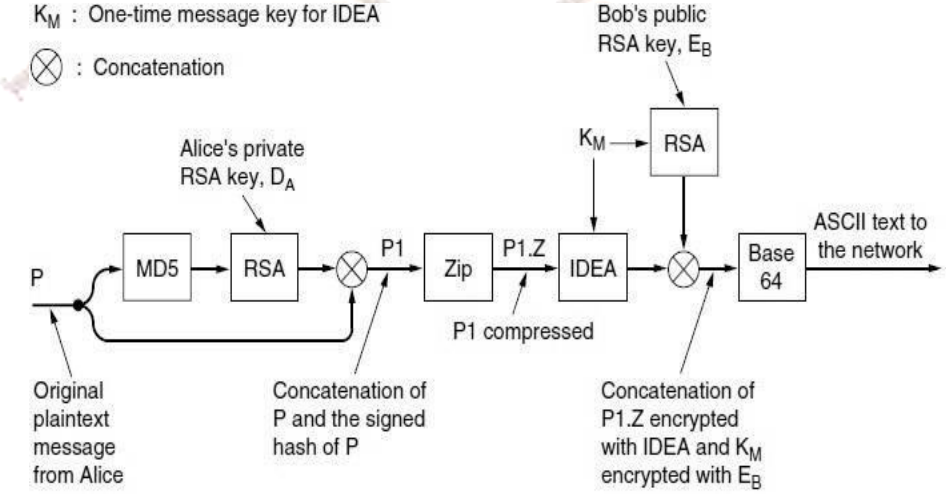

K_M : One-time message key for IDEA
⊗ : Concatenation
Bob's public RSA key, E_B
K_M
RSA
Alice's private RSA key, D_A
P
MD5
RSA
P1
Zip
P1.Z
IDEA
Base 64
ASCII text to the network
P1 compressed
Original plaintext message from Alice
Concatenation of P and the signed hash of P
Concatenation of P1.Z encrypted with IDEA and K_M encrypted with E_B

Fig 14.3: How PGP encryption works

Next, PGP prompts Alice for some random input. Both the content and the typing speed are used to generate a 128-bit IDEA message key, K_M. K_M is now used to encrypt *P1.Z* with IDEA in cipher feedback mode. In addition, K_M is encrypted with Bob's public key, E_B. These two components are then concatenated and converted to base64. When Bob gets the message, he reverses the base64 encoding and decrypts the IDEA key using his private RSA key. Using this key, he decrypts the message to get P1.Z. After decompressing it, Bob separates the plaintext from the encrypted hash and decrypts the hash using Alice's public key. If the plaintext hash agrees with his own computation, he knows that P is the correct message and that it came from Alice.

Key management is an important concept in PGP. It works as follows: each user maintains two data structures locally. They are a ***private key ring*** and a public key ring. The private key ring contains one or more personal private/public key pairs. Multiple pairs are supported per user to permit users to change their public keys periodically, without invalidating messages currently in preparation or in transit. Each pair has an identifier associated with it so that a message sender can tell the recipient which public key was used to encrypt it. Message identifiers consist of the low-order 64 bits of the public key. Users are themselves responsible for avoiding conflicts in their public-key identifiers. The private keys on disk are encrypted using a special password to protect them against hidden attacks.

The public key ring contains the public keys of the users. These are needed to encrypt the message keys associated with each message. Each entry on the public key ring contains the public key and its 64-bit identifier and an indication of how strongly the user trusts the key.

3.2 S/MIME

Secure/Multipurpose Internet Mail Extensions (S/MIME) is a standard for public key encryption and signing of MIME data. It provides authentication, data integrity, secrecy, and nonrepudiation. It also is quite flexible, supporting a variety of cryptographic algorithms. S/MIME integrates well with MIME, allowing all kinds of messages to be protected. A variety of new MIME headers are defined, for holding digital signatures. The general MIME specification defines the format and handling of e-mail attachments. S/MIME is the internet standard for secure e-mail attachments. S/MIME is similar to PGP and its predecessors, PEM (Privacy-Enhanced Mail). S/MIME has been adopted in commercial e-mail packages such as Eudora and Microsoft outlook.

The principal difference between S/MIME and PGP is the method of key exchange. Basic PGP depends on each user's exchanging keys with all potential recipients and establishing a ring of trusted recipients. It also requires establishing a degree of trust in the authenticity of the keys for those recipients. S/MIME uses hierarchically validated certificates, usually represented in X.509 format for key exchange. Thus, with S/MIME, the sender and recipient do not need to have exchanged keys in advance as long as they have a common certifier, they both trust. S/MIME works with a variety of cryptographic algorithms such as DES, AES and RC2 for symmetric encryption.

S/MIME performs security transformation very similar to those for PGP. PGP was originally designed for plaintext messages, but S/MIME handles all sorts of attachments such as data files. S/MIME is integrated into many commercial e-mail packages.

SELF-ASSESSMENT QUESTIONS – 2

7. __________________created PGP in 1991.
8. PGP encrypts data by using a block cipher called _________________.
9. contains one or more personal private/public key pairs.
10. is a standard for public key encryption and signing of MIME data.
11. The principal difference between S/MIME and PGP is the method of ______________

4. WEB SECURITY

We have discussed two important areas where security is needed, communications and email. Now we will discuss web security. The Web is the place where most of the threats are taking place nowadays. In the following sections, we will look at some of the problems and issues relating to web security. Website security can be divided into three parts.

They are: (i) secure naming, which describes how the objects and resources are named securely.
(ii) How can secure and authenticated connections be established?
(iii) What happens when a web site sends a client a piece of executable code? The following sections describes these three components of web security.

4.1 Secure Naming

Consider the situation where Alice wants to access Bob's web site, say www.blogs-bobs.com. She will type Bob's URL into her browser and wait for the page, after a few seconds the page appears. How she can make sure that the received page is actually Bob's web page. Suppose an intruder, says Trudy captures an HTTP GET request headed to Bob's Web site, she could go to Bob's Web site herself to get the page, modify it as she wishes, and return the fake page to Alice. In this case, Trudy has to be in a position to intercept Alice's outgoing traffic and forge her incoming traffic. In practice, she has to tap either Alice's phone line or Bob's but it is fairly difficult.

DNS Spoofing

One way of attack would be for Trudy to crack the DNS (Domain Name System) system or maybe just the DNS cache at Alice's ISP, and replace Bob's IP address (say, 36.1.2.3) with her (Trudy's) IP address (say, 42.9.9.9). Normal situation is shown in figure 14.4 (a). Figure 14.4 (b) shows the situation when an attack based on breaking into a DNS server and modifying Bob's record occurred. In this case, when Alice refers to Bob's IP address, she gets Trudy's and all the traffic sent by Alice, intended for Bob, goes to Trudy. In this way, Trudy can create a man-in-the-middle attack without having to go to the trouble of tapping any phone lines. Instead, she has to break into a DNS server and change one record.

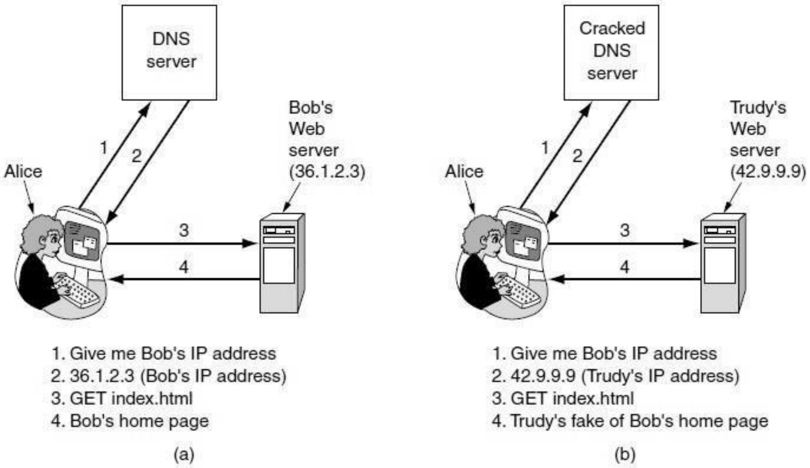

DNS server
Bob's Web server (36.1.2.3)
Alice
1
2
3
4
1. Give me Bob's IP address
2. 36.1.2.3 (Bob's IP address)
3. GET index.html
4. Bob's home page
(a)
Cracked DNS server
Trudy's Web server (42.9.9.9)
Alice
1
2
3
4
1. Give me Bob's IP address
2. 42.9.9.9 (Trudy's IP address)
3. GET index.html
4. Trudy's fake of Bob's home page
(b)

Fig 14.4: (a) Normal situation. (b) An attack based on breaking into a DNS server and modifying Bob's record.

This faking action takes place in such a way that Trudy can trick the DNS server at Alice's ISP into sending out a query to search Bob's address. Unfortunately, since DNS uses UDP, the DNS server has no way of checking who supplied the answer. Trudy can exploit this property by forging the expected reply and thus injecting a false IP address into the DNS server's cache.

Trudy starts the attack by sending a search request to Alice's ISP asking for the IP address of bob.com. Since there is no entry for this DNS name, the cache server queries the top-level server for the com domain to get one. However, Trudy beats the com server and sends back a false reply saying:

''bob.com is 42.9.9.9,'' (where 42.9.9.9 is Trudy's IP address). If her false reply gets back to Alice's ISP first, that one will be cached and the real reply will be rejected as an unrequested reply to a query no longer outstanding. Tricking a DNS server into installing a false IP address is called ***DNS spoofing***. A cache that holds an intentionally false IP address like this is called a ***poisoned cache.*** This type of spoofing is not that easy.

Secure DNS

The real issue is that DNS was designed during the initial stage of Internet, and that time security was not a major issue. Environment has changed by time, in 1994, IETF set up a working group to make DNS fundamentally secure. This project is known as DNSsec (DNS security). It is based on public-key cryptography. Every DNS zone has a public/private key pair. All information sent by a DNS server is signed with the originating zone's private key, so the receiver can verify its authenticity. DNSsec offers three fundamental services: proof of where the data originated, public key distribution, transaction and request authentication. The main service is the first one. It verifies that the data being returned has been approved by the zone's owner. The second one is useful for storing and retrieving public keys securely. The third one is needed to guard against playback and spoofing attacks.

DNS records are grouped into sets called **RRSets (Resource Record Sets),** with all the records having the same name, class, and type being chunked together in a set. Each RRSet is cryptographically hashed. The unit of transmission to clients is the signed RRSet. Upon receipt of a signed RRSet, the client can verify whether it was signed by the private key of the originating zone. If the signature agrees, the data is accepted.

DNSsec also provides a cryptographic mechanism to bind a response to a specific query, to prevent the kind of spoof Trudy managed to succeed in the previous example. This Anti-spoofing measure adds to the response a hash of the query message signed with the respondent's private key. Since Trudy does not know the private key of the top-level com server, she cannot forge a response to a query Alice's ISP sent there. She can certainly get her response back first, but it will be rejected due to its invalid signature over the hashed query.

4.2 SSL – The Secure Sockets Layer

SSL is a security protocol that was developed by Netscape Communications Corporation, along with RSA Data Security, Inc. The primary goal of the SSL protocol is to provide a private channel between communicating applications, which ensures privacy of data, authentication of the partners, and integrity.

SSL provides an alternative to the standard TCP/IP socket API that has security implemented within it. Therefore, in theory, it is possible to run any TCP/IP application in a secure way without changing the application. In practice, SSL is only widely implemented for HTTP connections, but Netscape Communications Corp has stated an intention to employ it for other application types, such as NNTP and Telnet, and there are several such implementations freely available on the Internet.

SSL is composed of two layers. The lower layer consists of a protocol for transferring data using a variety of predefined cipher and authentication combinations, called the *SSL Record Protocol.*

In reality, current implementations have the socket interface embedded within the application and do not expose an API that other applications can use. On the upper layer, there is a protocol for initial authentication and transfer of encryption keys which is called the *SSL Handshake Protocol.*

The SSL protocol is located at the top of the transport layer. SSL is also a layered protocol itself. It simply takes the data from the application layer, reformats it, and transmits it to the transport layer. An SSL session works in different states. These states are *session and connection states.* The SSL handshake protocol coordinates the states of the client and the server. In addition, there are read and write states defined to coordinate the encryption according to the *change CipherSpec* messages.

When both parties send a *change CipherSpec* message, it changes the pending write state to current write state. Again, when both parties receive a change CipherSpec message, it changes the pending read state to the current read state. Figure 14.6 illustrates an SSL handshake process.

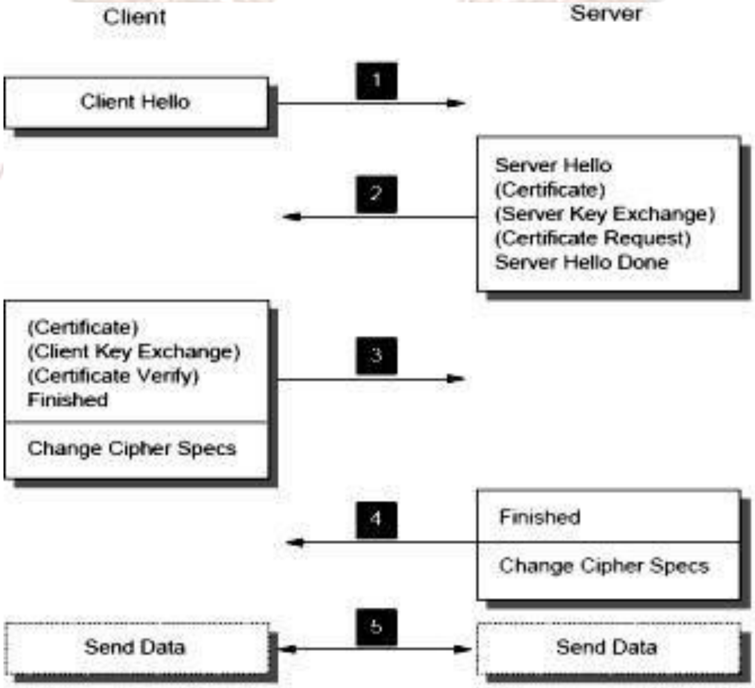


Fig 14.6: SSL Handshake process

The SSL handshake protocol allows the client and server to determine the required parameters for an SSL connection such as protocol version, cryptographic algorithms, optional client or server authentication, and public key encryption methods to generate shared secrets. During this process, all handshake messages are forwarded to the SSL record layer to be encapsulated into special SSL messages.

4.3 Mobile Code Security

Earlier, when Web pages were just static HTML files, they did not contain executable code. Now they often contain small programs, including Java applets, ActiveX controls, and JavaScripts. Downloading and executing such **mobile code** is clearly a massive security risk, so different methods have been invented to minimize the risk. The following section discusses some of the issues raised by mobile code and some approaches to deal with it.

Java Applet Security

Java applets are small Java programs compiled to a stack-oriented machine language called **JVM (Java Virtual Machine).** They can be placed on a web page for downloading along with the page. After the page is loaded, the applets are inserted into a JVM interpreter inside the browser.

The advantage of running interpreted code over compiled code is that each instruction is examined by the interpreter before being executed. It checks the validity of the address, system calls are also caught and interpreted. If an applet is trusted, its system calls could be carried out without question. However, if an applet is not trusted, it could be encapsulated in what is called a ***sandbox*** to restrict its behavior and trap its attempts to use system resources.

When an applet tries to use a system resource, its call is passed to a security monitor for approval. The monitor examines the call based on the local security policy and then makes a decision to allow or reject it. In this way, it is possible to give applets access to some resources but not all.

ActiveX

ActiveX controls are x86 binary programs that can be embedded in Web pages. When one of them is encountered, a check is made to see if it should be executed, and if it passes the test, it is executed. It is not interpreted or sandboxed, so it has as much power as any other user program, and can potentially do great harm. Thus, all the security is in the decision whether to run the ActiveX control.

The method that Microsoft chose for making this decision is based on the idea of ***code signing.*** Each ActiveX control is accompanied by a digital signature which is a hash of the code that is signed by its creator using public-key cryptography. When an ActiveX control turns up, the browser first verifies the signature to make sure it has not been manipulated with in transit. If the signature is correct, the browser then checks its internal tables to see if the program's creator is trusted or if there is a chain of trust back to a trusted creator. If the creator is trusted, the program is executed; otherwise, it is not. The Microsoft system for verifying ActiveX controls is called *Authenticode.*

Javascript

JavaScript does not have any formal security model, but it does have a long history of leaky implementations. Each vendor handles security in a different way. For example, Netscape Navigator version 2 used something akin to the Java model, but version 4 that had been abandoned for a code-signing model. The fundamental problem is that letting foreign code run on your machine is asking for trouble. If something unexpected happens and the user is distracted for a moment, it will create a security risk.

Browser Extensions

Browser extensions are computer programs that extend the functionality of Web browsers. Plug-ins often provide the capability to interpret or display a certain type of content, such as PDFs or Flash animations. Extensions and add-ons provide new browser features, such as better password management, or ways to interact with pages.

Installing an extension, add-on, or plug-in is very simple. All of these programs are written to frameworks that differ depending on the browser that is being enhanced. There are two failure modes in case of browser extensions. The first is that the program may behave maliciously. The second problem is that plug-ins give the browser the ability to interpret new types of content. For all of these reasons, add-ons and plug-ins should only be installed as needed and only from trusted vendors.

Viruses

Viruses are another form of mobile code. The difference between a virus and ordinary mobile code is that viruses are written to reproduce themselves. When a virus arrives, either via a Web page, an email attachment, or some other way, it usually starts out by infecting executable programs on the disk. When one of these programs is run, control is transferred to the virus, which usually tries to spread itself to other machines.

Viruses have become a huge problem on the Internet and have caused billions of dollars' worth of damage. There is no clear solution. Possibly, a whole new generation of operating systems based on secure microkernels and tight compartmentalization of users, processes, and resources might help to overcome this.

A botnet attack is a type of cyber-attack carried out by a group of internet-connected devices controlled by a malicious actor.

Botnets themselves are simply a network of devices. It is when cyber criminals inject malware into the network to control them as a collective that they get used to launching cyber-attacks. Botnet attacks can be used for sending spam, data theft, compromising confidential info, perpetuating ad fraud or for launching more dangerous Distributed Denial of Service or DDoS attacks.

- Botnet attacks start with cyber criminals gaining access to devices by compromising their security.
- They could do this via hacks like the injection of Trojan viruses or basic social engineering tactics. Then these devices are brought under control using software that commands the devices to carry out attacks on a large scale.
- Sometimes, the criminals themselves may not use the botnet to launch attacks but instead, they sell access to the network to other malicious actors. These third parties can then use the botnet as a "zombie" network for their own needs, like directing spam campaigns.

Different Types of Botnets

- Distributed Denial-of-Service (DDoS) attacks: One of the more common types of botnet attacks which work by overloading a server with web traffic sent by bots in order to crash it. This downtime in the server's operation can also be used for launching additional botnet-based attacks.

- Phishing attacks: These are often launched with the purpose of extracting key information from an organization's employees. For example, mass spam campaigns can be devised to imitate trusted sources within the organization to trick people into revealing confidential information like login details, financial info and credit card details.
- Brute force attacks: These involve programs which forcefully breach web accounts by force. Dictionary attacks and credential stuffing are used to exploit weak user passwords and access their data.

Types of Web-based Attacks

- Injection attacks
- DNS spoofing
- Session hijacking
- Phishing
- Brute force
- Denial of service
- Dictionary attacks
- URL interpretation
- File inclusion attacks
- Man in the middle attacks

Web security tools

- Firewalls
- Anti-virus software
- MDR service
- Staff training
- PKI service
- Penetration testing

SELF-ASSESSMENT QUESTIONS – 3

12. Tricking a DNS server into installing a false IP address is called ________________.
13. A cache that holds an intentionally false IP address like this is called a ________________.
14. DNS records are grouped into sets called __________________.
15. The primary goal of the _________________ protocol is to provide a private channel between communicating applications, which ensures privacy of data, authentication of the partners, and integrity.

5. SUMMARY

Let us recapitulate the important concepts discussed in this unit:

- Internet Protocol Security (IPSec) is a protocol suite for securing communications using internet protocol (IP) by authenticating and encrypting each IP packet of a communication.
- IPSec can be used in two modes. They are transport mode and tunnel mode.
- Firewall is a network security system to prevent unauthorized access by controlling the incoming and outgoing traffic.
- PGP is a complete email security package that provides privacy, authentication, digital signatures, and compression.
- Secure/Multipurpose Internet Mail Extensions (S/MIME) is a standard for public key encryption and signing of MIME data.
- The principal difference between S/MIME and PGP is the method of key exchange.
- Tricking a DNS server into installing a false IP address is called DNS spoofing.
- A cache that holds an intentionally false IP address like this is called a poisoned cache.
- DNS records are grouped into sets called RRSets (Resource Record Sets), with all the records having the same name, class, and type being chunked together in a set.
- Java applets are small Java programs compiled to a stack-oriented machine language called JVM (Java Virtual Machine).
- ActiveX controls are x86 binary programs that can be embedded in Web pages.

6. TERMINAL QUESTIONS

1. Explain IP Security (IPSec).
2. What is the use of firewall? Explain.
3. Describe Virtual Private Networks.
4. Explain Pretty Good Privacy.
5. Describe S/MIME.
6. Write short notes on web security.

7. ANSWERS

Self-Assessment Questions

1. Internet Protocol (IP)
2. Transport mode, tunnel mode
3. (a) True
4. Stateful firewalls
5. Virtual Private Networks (VPN)
6. WEP (Wired Equivalent Privacy)
7. Phil Zimmermann
8. IDEA (International Data Encryption Algorithm)
9. Private key ring
10. S/MIME
11. Key Exchange
12. DNS Spoofing
13. Poisoned cache
14. RR Sets
15. SSL

Terminal Questions

1. Internet Protocol Security (IPSec) is a protocol suite for securing communications using internet protocol (IP) by authenticating and encrypting each IP packet of a communication. The complete IPSec design is a framework for multiple services such as secrecy, data integrity and protection from replay attacks. Even though IPSec is in the IP layer, it is connection oriented... (Refer section 2.1 for more details).

2. Firewall is a network security system to prevent unauthorized access by controlling the incoming and outgoing traffic. Firewall acts as a packet filter. It checks all the incoming and outgoing packets... (Refer section 2.2 for more details).
3. When public data networks and the internet appeared, many companies wanted to move their data to public network, without compromising the security of private network. This led to the invention of VPNs (Virtual Private Networks), which overlay networks on top of public networks but with most of the properties of private networks... (Refer section 2.3 for more details).
4. Phil Zimmermann created PGP in 1991. PGP is a complete email security package that provides privacy, authentication, digital signatures, and compression. The complete package, including all the source code, is distributed free on the Internet. Due to its quality, zero cost, and easy availability on UNIX, Linux, Windows, and Mac OS platforms, it is widely used today... (Refer section 3.1 for more details).
5. Secure/Multipurpose Internet Mail Extensions (S/MIME) is a standard for public key encryption and signing of MIME data. It provides authentication, data integrity, secrecy, and nonrepudiation... (Refer section 3.2 for more details).
6. Website security can be divided into three parts. They are: Secure naming, which describes how the objects and resources are named securely. Second, how can secure and authenticated connections be established? And third, what happens when a web site sends a client a piece of executable code… (Refer section 4 for more details)

References

1. Andrew S Tanenbaum, David J.Wetherall, *“Computer Networks,”* Fifth edition.
2. Larry L. Peterson, Bruce S. Davie, *“Computer Networks- a Systems Approach,”* Fifth edition.
3. James F. Kurose, Keith W.Ross, *“Computer Networking-A top-down approach,”* Sixth edition.
4. Behrouz A.Forouzan, Sophia Chung Fegan, *“Data Communication and Networking,”* Fourth edition.
5. William Stallings*, “Computer Networking with Internet Protocols and Technology,”* Third edition.