Unit 2
E-MAIL SECURITY & FIREWALLS

Chamundeswari Arumugam
Professor
SSN College of Engineering, Chennai

AUGUST 2017

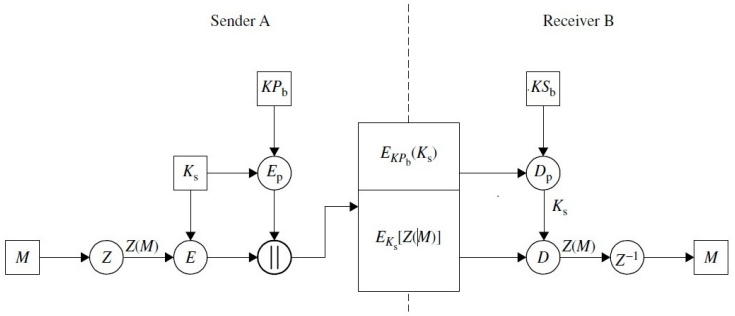
Outline

- PGP
  - Confidentiality
  - Authentication
  - Radix-64 conversion
  - Packet header
  - Key material packet
  - Packet structure
- S/MIME
  - MIME- Introduction description MIME header Security multiparts MIME security with OpenPGP
  - S/MIME - Introduction, Definitions, CMS options
  - Enchanced security services for S/MIME - Introduction, triple wrapped message, security services with triple wrapping.
- Firewall
  - Introduction
  - Role of firewalls
  - Firewall realted terminology
  - Types of firewalls
  - Firewall designs
- SET
  - Introduction
  - Basic requirement for SET
  - SET system participants
  - Crytographic operation principles
  - Authentication and message integrity
  - Dual signature and Signature verification
  - Payment processing

PGP

- Pretty Good Privacy (PGP) was invented by Philip Zimmermann who released version 1.0 in 1991.
- It also provides data integrity services for messages and data files by using digital signature, encryption, compression (zip) and radix-64 conversion.

Fig : PGP confidentiality computation scheme



Confidentiality via Encryption

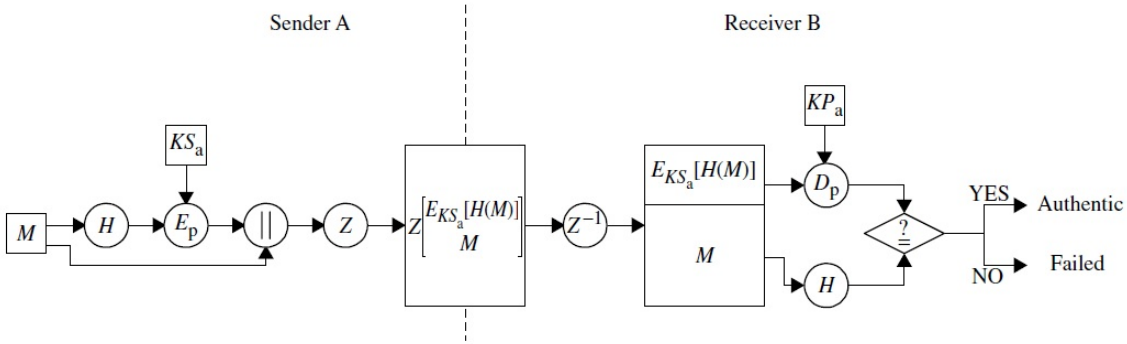
- The sender creates a message.
- The sending PGP generates a random 128-bit number to be used as a session key for this message only.
- The session key is encrypted with RSA, using the recipients public key.
- The sending PGP encrypts the message, using CAST-128 or IDEA or 3DES, with the session key. Note that the message is also usually compressed.
- The receiving PGP uses RSA with its private key to decrypt and recover the session key.
- The receiving PGP decrypts the message using the session key. If the message was compressed, it will be decompressed.

The Notation

- K_s = session key, || = concatenation
- KP_a = public key of user A
- KS_a = private key of user A
- E = conventional encryption, D = conventional decryption
- E_p = public-key encryption
- Z = compression using zip algorithm
- H = hash function
- KP_b = public key of user B
- KS_b = private key of user B
- D_p = public-key decryption
- Z^{-1} = decompression

PGP (Contd..)

Fig : PGP authentication computation scheme using compression algorithm



Authentication via Digital Signature

- The sender creates a message.
- SHA-1 is used to generate a 160-bit hash code of the message.
- The hash code is encrypted with RSA using the senders private key and a digital signature is produced.
- The binary signature is attached to the message.
- The receiver uses RSA with the senders public key to decrypt and recover the hash code.
- The receiver generates a new hash code for the received message and compares it with the decrypted hash code. If the two match, the message is accepted as authentic.

Compression

- PGP compresses the message after applying the signature but before encryption.
- Save space - e-mail transmission & file storage.
- Trade-offs to produce compressed forms - running speed versus compression ratio. Types are as follows :
  1. ZIP
  2. Abraham Lempel (1977)
  3. Jakob Ziv (1978)
  4. LZSS (1982), based on the work of Lempel and Ziv.
  5. dynamic Huffman coding (LZH)
  6. ShannonFano coding (ZIP 1.x).
  7. LZ77 and LZ78 to produce a hybrid called LZFG.
- Decompression of LZ77-compressed text is simple and fast.

PGP (Contd..)

Radix-64 Conversion

- The block to be transmitted is encrypted.
- Resulting block consists of a stream of arbitrary 8-bit octets.
- convert the raw 8-bit binary octets to a stream of printable 7-bit ASCII characters, called radix-64 encoding or ASCII Armor.
- Example : A 24-bit input block to 32 bit block
- 10110010 01100011 00101001
- hexadecimal representation : is b2 63 29.
- Arrange the input block in 6 bits : 101100 100110 001100 101001
- Yields 6-bit decimal values - 44, 38, 12, 41
- the radix-64 (using table) :smMp
- ASCII format : 73 6d 4d 70
- Binary representation : 01110011 01101101 01001101 01110000

Radix-64 Conversion-Encoding Binary in Radix-64

- The encoding process represents three 8-bit input groups as output strings of four encoded characters.
- Radix-64 printable encoding of binary data is shown in Figure (a)

6-bit value	Character encoding	6-bit value	Character encoding	6-bit value	Character encoding	6-bit value	Character encoding
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/
						(pad)	=

Table. Radix-64 encoding

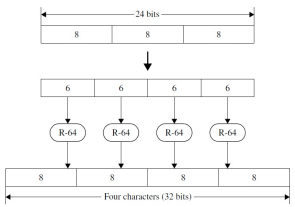


Fig (a) Radix-64 printable encoding of binary data

Radix-64 Conversion - ASCII Armor Format

- PGP encodes data into ASCII Armor, it puts specific headers around the data :
  1. An Armor head line : BEGIN PGP MESSAGE, BEGIN PGP PUBLIC KEY BLOCK, BEGIN PGP PRIVATE KEY BLOCK, BEGIN PGP MESSAGE, PART X/Y, BEGIN PGP MESSAGE, PART X, BEGIN PGP SIGNATURE
  2. Armor headers: Version, Comment, MessageID, Hash, Charset,
  3. A blank line
  4. ASCII-Armoured data
  5. Armour checksum
  6. Armour tail

PGP (Contd..)

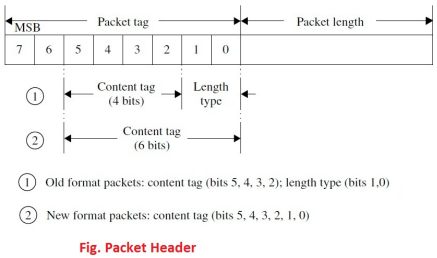


Fig. Packet Header

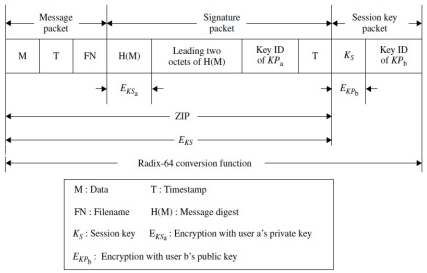


Fig. PGP Message Format

Packet Headers

- Packet tag : The packet tag denotes what type of packet the body holds.Old format packets: content tag (bits 5, 4, 3, 2); length type (bits 1,0). New format packets: content tag (bits 5, 4, 3, 2, 1, 0).

Key Material Packet

- A key material packet contains all the information about a public or private key.
- Depends on packet header format.
- Key Packet Variants : Public-key packet, Public subkey packet, Secret-key packet, Secret-subkey packet
- Public-key & public subkey Packet Formats : Provide signature and encrpytion service
- Secret-key Packet Formats : The secret-key and secret-subkey packets contain all the data of public-key and public subkey packets in encrypted form, with additional algorithm-specific key data appended.

Packet Structure

- Message Packet : actual data to be transmitted.
- Signature Packet :
  - This packet describes a binding between some public key and some data.
  - Two versions of signature packets are defined.Ver 3 and Ver 4.
  - Ver 3 include the components : timestamp, message digest, Leading two octets of hash code, Key ID of senders public key.
  - The signature calculation for version 4 signature is based on a hash of the signed data.
- Session Key Packets : This component includes the session key and the identifier of the receivers public key that was used by the sender to encrypt the session key.

Service	**Algorithm**
Public-Key Alg	RSA, ElGamal,DSA
Symmetric-Key Alg	IDEA, Triple DES, CAST 5
Compression Alg	ZIP, ZLIB
Hash Alg ID	MD5, SHA-1

MIME

- **Introduction**
  1. Secure/Multipurpose Internet Mail Extension (S/MIME) provides a consistent means to send and receive secure MIME data.
  2. SMTP sends messages only in NVT (Network Virtual Terminal) 7-bit ASCII format.
  3. MIME was defined to allow transmission of non-ASCII data through e-mail.
  4. MIME is not a mail protocol and cannot replace SMTP; it is only an extension to SMTP.
  5. Each MIME message includes information that tells the recipient the type of the data and the encoding used.

MIME

- **Description**
  1. MIME transforms non-ASCII data at the senders site to NVT ASCII data and delivers it to the client SMTP to be sent through the Internet.
  2. The server SMTP at the receivers site receives the NVT ASCII data and delivers it to MIME to be transformed back to the original non-ASCII data.
  3. Figure illustrates this concept.

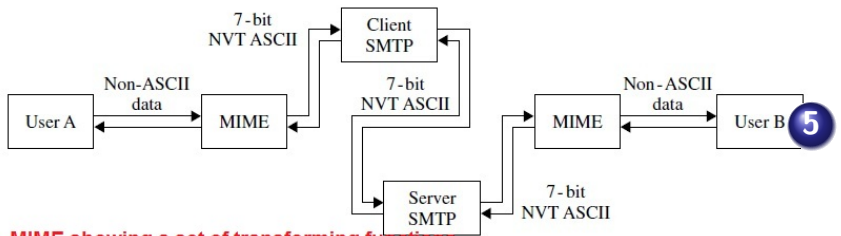


Fig. MIME showing a set of transforming functions.

MIME

- **MIME header**
  1. MIME Version : defines the version of MIME used
  2. Content Type : defines the 7 type of data used in the message body. Text, multipart, message, image, video, audio, application.
  3. Content Transfer Encoding : defines five types of encoding the msg into ones and zeros for transport. 7 bit, 8 bit, binary, Base64 and Quoted-printable
  4. Content Id : identifies the whole msg in a multiple msg environment:
  5. Content Description : defines whether the body is image, audio or video

S/MIME (contd..)

MIME

- **Security Multiparts**
  1. Basic MIME by itself does not specify security protection.
  2. MIME agent must provide security services by employing a security protocol
  3. Define two security subtypes of the MIME multipart content type: signed and encrypted
  4. The multipart/signed content type specifies how to support authentication and integrity services via digital signature.
  5. The multipart/encrypted content type specifies how to support confidentiality via encryption.

MIME

- **MIME Security with OpenPGP**
  1. OpenPGP message format can be used to provide privacy and authentication using the MIME security content type
  2. OpenPGP encrypted data is denoted by the multipart/encrypted content type,
  3. OpenPGP signed messages are denoted by the multipart/signed content type
  4. OpenPGP digital signature is generated
  5. OpenPGP packet format describes a method for signing and encrypting data in a single OpenPGP message

S/MIME

- **Introduction**
  1. S/MIME provides a way to send and receive 7-bit MIME data.
  2. The S/MIME agent represents user software that is a receiving agent, a sending agent, or both.
  3. S/MIME agents must use the Internet X.509 Public-Key Infrastructure (PKIX) certificates to validate public keys

S/MIME

- **Definitions**
  1. ASN.1, BER, DER, Certificate, CRL, Attribute certificate, Sending agent, Receiving agent, S/MIME agent

S/MIME (contd..)

S/MIME

- **Cryptographic Message Syntax (CMS) Options**
  1. CMS provides additional details regarding the use of the cryptographic algorithms.
  2. DigestAlgorithmIdentifier : SHA-1, MD5
  3. SignatureAlgorithmIdentifier : id-dsa, rsaEncryption
  4. KeyEncryptionAlgorithmIdentifier : DiffieHellman key exchange, rsaEncryption.
  5. General syntax : support six different content types: data, signed data, enveloped data, signed-and-enveloped data, digested data and encrypted data.

Enhanced Security Services for S/MIME

- **Introduction**
  1. Service use triple wrapped message (TWM)
  2. TWM is one that has been signed, then encrypted and then signed again.
  3. Inside signature is used for content integrity
  4. Encrypted body - confidentiality, including confidentiality of the attributes that are carried in the inside signature.
  5. Outside signature provides authentication and integrity for information

Enhanced Security Services for S/MIME

- **Triple wrapped msg**
  1. Create a triple wrapped message
  2. A triple wrapped message has many layers of encapsulation

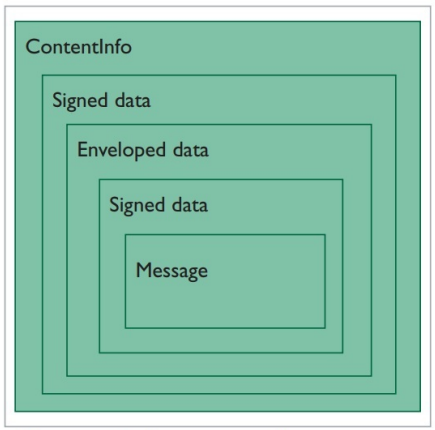


Figure. Triple-wrapped message.

Enhanced Security Services for S/MIME

- **Security Services with Triple Wrapping**
  1. If a signed receipt is requested for a triple wrapped message, the receipt request must be in the inside signature, not in the outside signature

Internet Firewalls for Trusted Systems

Introduction

- A firewall is a device or group of devices that controls access between networks.
- It consists of filters and gateway(s).It is an agent which screens network traffic.Protect the intranet from Internet-based attacks
- It act as an intermediate server in handling SMTP and HTTP connections in either direction.
- Classified into three main categories: packet filters, circuit-level gateways and application-level gateways.

Role of Firewalls

- It imposes restrictions on packets entering or leaving the private network.Packets are not allowed through unless they conform to a filtering specification.
- It create checkpoints (or choke points) between an internal private network and an untrusted Internet.
- It may filter on the basis of IP source and destination addresses and TCP port number.
- It control access at the application layer, using user identification as the criterion.
- Firewalls for ATM networks may control access based on the data link layer criteria.
- By placing logging services at firewalls, security administrators can monitor all access to and from the Internet.

Role of Firewalls(contd..)

- They also block SMTP and FTP connections to the Internet from internal systems not authorised to send e-mail or to move files.
- Provides protection from various kinds of IP spoofing and routing attacks.
- Using the tunnel mode capability, the firewall can be used to implement Virtual Private Networks (VPNs)
- Can effectively implement and control the traversal of IP multicast traffic.
- Negative aspects: unable to protect against the transfer of virus-infected programs or files.

Firewall-Related Terminology

- **Bastion host**
  - It is a publicly accessible device for the networks security.
  - It serves as a platform for any one of the 3 types of firewalls: packet filter, circuit-level gateway or application-level gateway.
  - Bastion hosts are armed with logging and alarm features to prevent attacks.
  - Bastion hosts role falls into the following three common types : Single-homed bastion host, Dual-homed bastion host, Multihomed bastion host, tri-homed firewall.

Internet Firewalls for Trusted Systems(Contd..)

Firewall-Related Terminology(Contd..)

- **Proxy Server**
  - Proxy servers are used to communicate with external servers on behalf of internal clients.
  - Application proxies forward packets only when a connection has been established
  - When the connection closes, a firewall using application proxies rejects individual packets, even if they contain port numbers allowed by a rule set.
  - The audit log is an essential tool for detecting and terminating intruder attacks.
  - proxy module is a relatively small software package specifically designed for network security.
  - Each proxy is independent of other proxies on the bastion host. If there is a problem with the operation of any proxy, or if future vulnerability is discovered, it is easy to replace the proxy without affecting the operation of the proxys applications.

Firewall-Related Terminology (Contd..)

- **Socks**
  - The SOCKS protocol version 4 provides for unsecured firewall traversal for TCP-based client/server applications, including HTTP, TELNET and FTP
  - When a TCP-based client wishes to establish a connection to an object that is reachable only via a firewall, it must open a TCP connection to the appropriate SOCKS port on the SOCKS server system.
  - The SOCKS server evaluates the request, and either establishes the appropriate connection or denies it.
  - It does not provide a clear-cut solution to the problem of encrypting the data traffic

Firewall-Related Terminology (Contd..)

- **Choke Point**
  - A choke point is the point at which a public internet can access the internal network.
  - A monitoring tools should be configured on the choke points
  - Choke points have been clearly established, the firewall devices can monitor, filter and verify all inbound and outbound traffic
  - Choke point is installed at the firewall, a prospective hacker will go through the choke point.

Internet Firewalls for Trusted Systems(Contd..)

Firewall-Related Terminology(Contd..)

- **De-militarised Zone (DMZ)**
  - DMZ is a network that lies between an internal private network and the external public network
  - sometimes called perimeter networks
  - The internal filter is used to guard against the consequences of a compromised gateway, while the outside filter can be used to protect the gateway from attack.

Firewall-Related Terminology (Contd..)

- **VPN**
  - VPNs are appropriate for any organisation requiring secure external access
  - VPNs are tunnelling protocols
  - The VPN encapsulates all the encrypted data within an IP packet.
  - Authentication, message integrity and encryption are very important fundamentals for implementing a VPN.

Firewall-Related Terminology (Contd..)

- **Logging and Alarms**
  - Logging is usually implemented at every device in the firewall
  - Logging devices will probably capture all hacker activities, including all user activities as well. The user can then tell exactly what a hacker is doing, and have such information available for audit.
  - Audit log is an essential tool for detecting and terminating intruder attacks.
  - Firewall should alert the user.
  - Two most common actions : to break the TCP/IP connection, set off alarms

Types of Firewalls

- **Circuit level gateways**
  - The circuit-level gateway represents a proxy server that statically defines what traffic will be forwarded. It forward packets containing a given port number
  - They operate at the network level of the OSI model.
  - Advantage of a proxy server is its ability to provide NAT.
  - Works on the same principles as packet filter firewalls

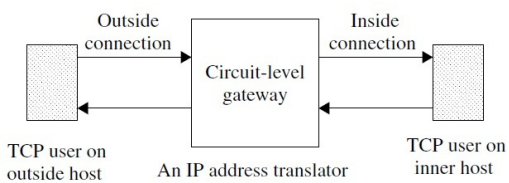


Fig. Circuit-level gateway for setting up two TCP connections.

Internet Firewalls for Trusted Systems(Contd..)

Types of firewall (Contd..)

- **Packet filters**
- Process network traffic on a packet-by-packet basis.
- A packet filter is a device which inspects or filters each packet at a screening router for the content of IP packets.
- The type of router used in a packet-filtering firewall is known as a screening router. Fig (a) illustrates.
- Packet filters typically set up a list of rules.
- A packet filter will provide two actions, forward or discard. If all the rules are met, then forward action will route the packet as normal, else discard action will block all packets.
- packet filters cannot tell whether the routed packet contains good or malicious data.
- Another weakness of packet filters is their susceptibility to spoofing.

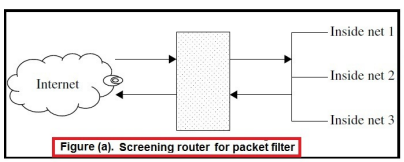


Figure (a). Screening router for packet filter

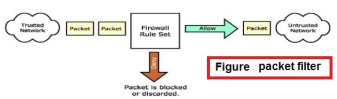


Figure packet filter

Table (a) Telnet packet-filtering example

Rule number	Action	Source IP	Source port	Destination IP	Destination port	Protocol
1	Discard	*	23	*	*	TCP
2	Discard	*	*	*	23	TCP

Table (b) FTP Packet Filtering Example

Rule number	Action	Source IP	Source port	Destination IP	Destination port	Protocol
1	Allow	192.168.10.0	*	*	21	TCP
2	Block	*	20	192.168.10.0	<1024	TCP
3	Allow	*	20	192.168.10.0	*	TCP ACK = 1

Types of Firewall (Contd..)

- **Packet filtering - TELNET**
- TELNET is a simple remote terminal access that allows a user to log onto a computer across an internet.
- TELNET client software allows the user to specify a remote machine either by giving its domain name or IP address.
- TELNET runs on TCP port 23.Tabe(a) represent the TELNET connection rule set.
- It runs in open non-encryption, with no authentication

Types of Firewalls (Contd..)

- **Packet filter - FTP**
- Packet filter allow or block FTP service using TCP ports 20 and 21.
- FTP is the first protocol for transferring or moving files across the Internet
- FTP was not designed with security in mind.
- Each FTP server has a command channel, where the requests for data and directory listings are issued, and a data channel, over which the requested data is delivered.
- FTP operates in two different modes (active and passive).
- Tabe(b) represent the FTP connection rule set.

Internet Firewalls for Trusted Systems(Contd..)

Types of firewall (Contd..)

- **Packet filters - SMTP**
- On the Internet, e-mail exchanges between mail servers are handled with SMTP.
- A hosts SMTP server accepts mail and examines the destination IP address to decide whether to deliver the mail locally or to forward it to some other machine.
- SMTP receivers use TCP port 25; SMTP senders use a randomly selected port above 1023.
- SMTP server uses DNS (Directory and Naming Services) to determine the matching IP address.
- Sendmail (www.sendmail.org/) is the mailer commonly used on UNIX systems.
- Sendmail is very actively supported on security issues, and has both an advantage and a disadvantage.

Table. (a) SMTP packet-filtering examples

Case	Action	Source host	Source port	Destination host	Destination port	Protocol
A	Allow	Source gateway	25	*	*	TCP
B	Allow	*	*	*	25	TCP
C	Allow	Internal host	*	*	25	TCP
D	Allow	*	25	*	*	TCP ACK flag

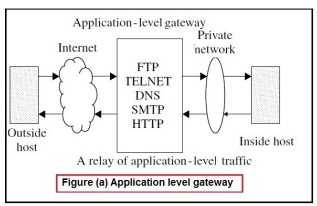
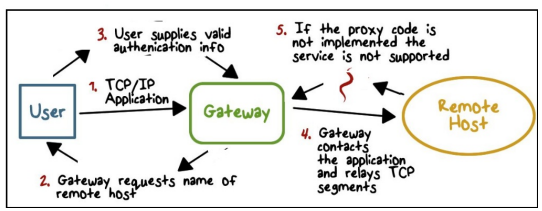


Figure (a) Application level gateway

Table. (b) SMTP packet-filtering examples-1

Rule	Direction	Source Address	Dest. Address	Protocol	Source Port	Dest. Port	Action
A	In	External	Internal	TCP	> 1023	25	Permit
B	Out	Internal	External	TCP	25	> 1023	Permit
C	Out	Internal	External	TCP	> 1023	25	Permit
D	In	External	Internal	TCP	25	> 1023	Permit
E	Either	Any	Any	Any	Any	Any	Deny



Types of Firewall (Contd..)

- **Application-Level Gateways**
- The application-level gateway represents a proxy server, performing at the TCP/IP application level
- Application proxies forward packets only when a connection has been established
- Connection closes, a firewall using application proxies rejects individual packets, even if the packets contain port. numbers allowed by a rule set.
- When an inside host initiates a TCP/IP connection, the application gateway receives the request and checks it against a set of rules or filters.
- The application gateway (or proxy server) will then initiate a TCP/IP connection with the remote server.
- If the remote servers response is permitted, the proxy server will then forward the response to the inside host
- The proxy server must analyse each UDP packet and apply it to the filters separately, which slows down the proxy process
- ICMP programs are nearly impossible to proxy because ICMP messages do not work through an application-level gateway.
- Application gateways (proxy servers) are used as intermediate devices when routing SMTP traffic to and from the internal network and the Internet.
- Main advantage of a proxy server is its ability to provide NAT for shielding the internal network from the Internet.

Internet Firewalls for Trusted Systems(Contd..)

Firewall Designs

- **Introduction**
  - Concerns how to implement a firewall strategy
  - Prevent the firewall devices from being compromised by threats
  - Three basic firewall designs : a single-homed bastion host, a dual-homed bastion host and a screened subnet firewall.
  - A single-homed bastion host, a dual-homed bastion host and a screened subnet firewall.
  - When Internet users attempt to access resources on the Internet network, the first device they encounter is a bastion host.
  - Bastion hosts must check all incoming and outgoing traffic and enforce the rules specified in the security policy.
  - Armed with logging and alarm features to prevent attacks

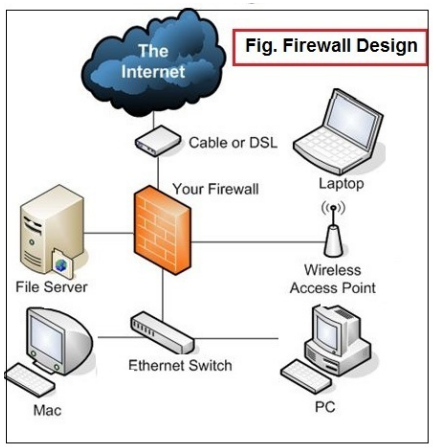


Fig. Firewall Design

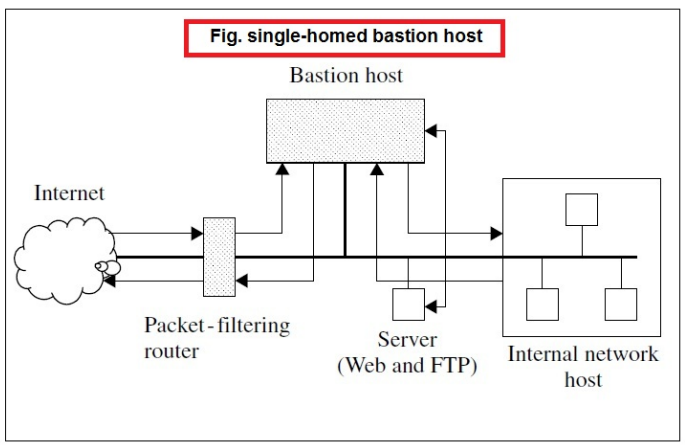


Fig. single-homed bastion host

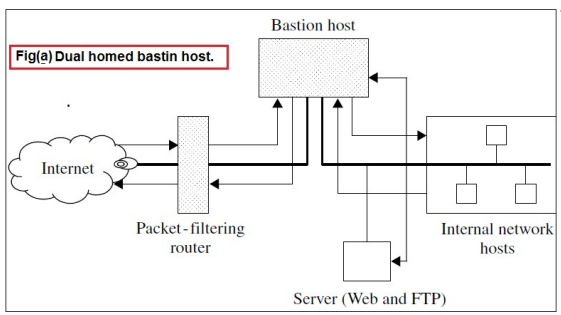
Firewall Designs (Contd..)

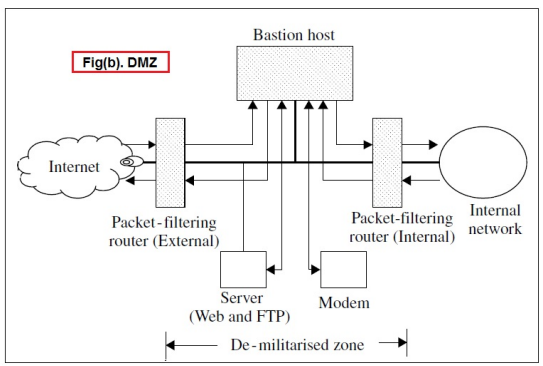
- **Screened Host Firewall (Single-Homed Bastion Host)**
  - Configured as either circuit-level or application-level gateways
  - NAT is essentially needed for developing an address scheme internally
  - It translates the internal IP addresses to IANAregistered addresses to access the Internet.
  - The screened host firewall is designed such that all incoming and outgoing information is passed through the bastion host.
  - The external screening router is configured to route all incoming traffic directly to the bastion host as indicated in Figure
  - The screening router is also configured to route outgoing traffic only if it originates from the bastion host.
  -
  - But such a bypass usually does not happen because a network using a single-homed bastion host is normally configured to send packets only to the bastion host, and not directly to the Internet.

Internet Firewalls for Trusted Systems(Contd..)

Firewall Designs

- **Screened Host Firewall(Dual-Homed Bastion Host)**
  - The configuration of the screened host firewall using a dual-homed bastion host adds significant security, compared with a single-homed bastion host.
  - It has two interfaces.
  - It creates a complete break between the internal network and the external Internet.
  - A hacker may try to subvert the bastion host and the router to bypass the firewall mechanisms. A dual-homed bastion host removes even this possibility.
  - Possible to implement NAT for dual-homed bastion hosts.





Firewall Designs (Contd..)

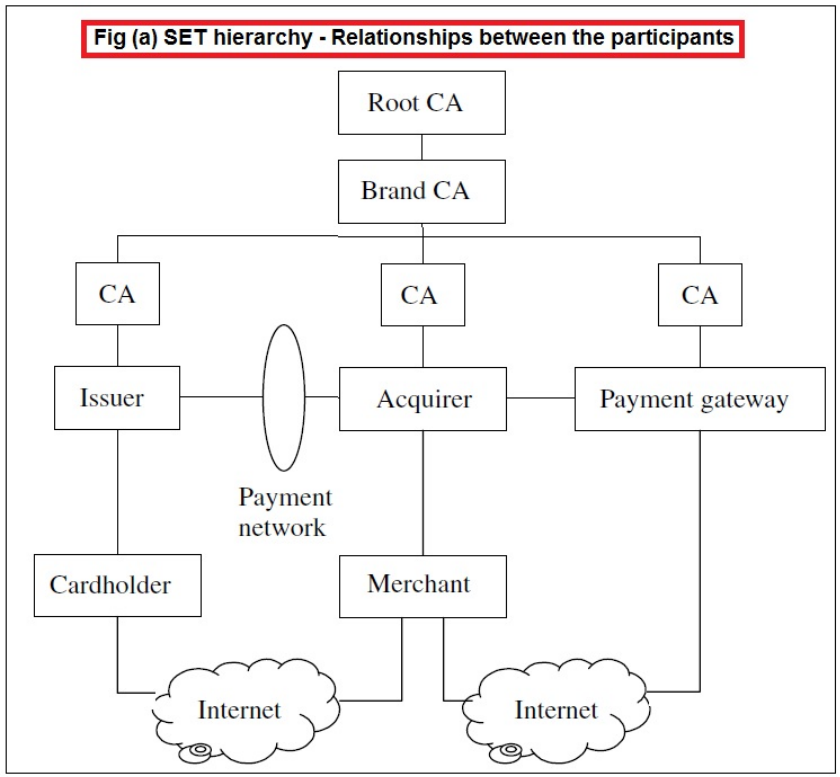
- **Screened Subnet Firewall**
  - DMZ firewall is the most secure one because it uses a bastion host to support both circuit- and application-level gateways.
  - DMZ functions as a small isolated network positioned between the Internet and the internal network.
  - It contains external and internal screening routers.
  - External and internal screening router prevent attacks such as IP spoofing and source routing.
  - The external screening router uses standard filtering to restrict external access to the bastion host, and rejects any traffic that does not come from the bastion host.
  - Internal router rejects incoming packets that do not originate from the bastion host, and sends only outgoing packets to the bastion host.
  - Benefits -tri-homed interfaces, internal network, internal users cannot access the Internet without going through the bastion host.

SET for E-commerce Transactions

- The Secure Electronic Transaction (SET) is a protocol designed for protecting credit card transactions over the Internet.
- SET relies on cryptography and X.509 v3 digital certificates to ensure message confidentiality and security.

Business Requirements for SET

- Confidentiality of information
- Integrity of data
- Cardholder account authentication
- Merchant authentication
- Security techniques
- Creation of brand-new protocol-SET
- Interoperability



SET System Participants

- Cardholder, Issuer, Merchant, Acquirer, Payment gateway, Certification Authority
- Figure (a) illustrates the SET hierarchy which reflects the relationships between the participants in the SET system

Cryptographic Operation Principles

- Confidentiality, Integrity(digital signature), Authentication (Certificate Authority)

SET for E-commerce Transactions(Contd..)

Authentication and Message Integrity

- Encryption process: plaintext, message digest, digital signature, random symmetric key, digital envelope
- Decryption process : encrypted message, digital envelope, symmetric key, digital signature, message digest, new message digest, compares his or her message digest to the one obtained from As digital signature.

Dual Signature and Signature Verification

- A dual signature is generated by creating the message digest of two messages: order digest and payment digest.
- The customer takes the hash codes (message digests) of both the order message and payment message by using the SHA-1 algorithm.
- These two hashes, ho and hp, are then concatenated and the hash code h of the result is taken.
- Finally, the customer encrypts (via RSA) the final hash code with his or her private key, Ksc, creating the dual signature.

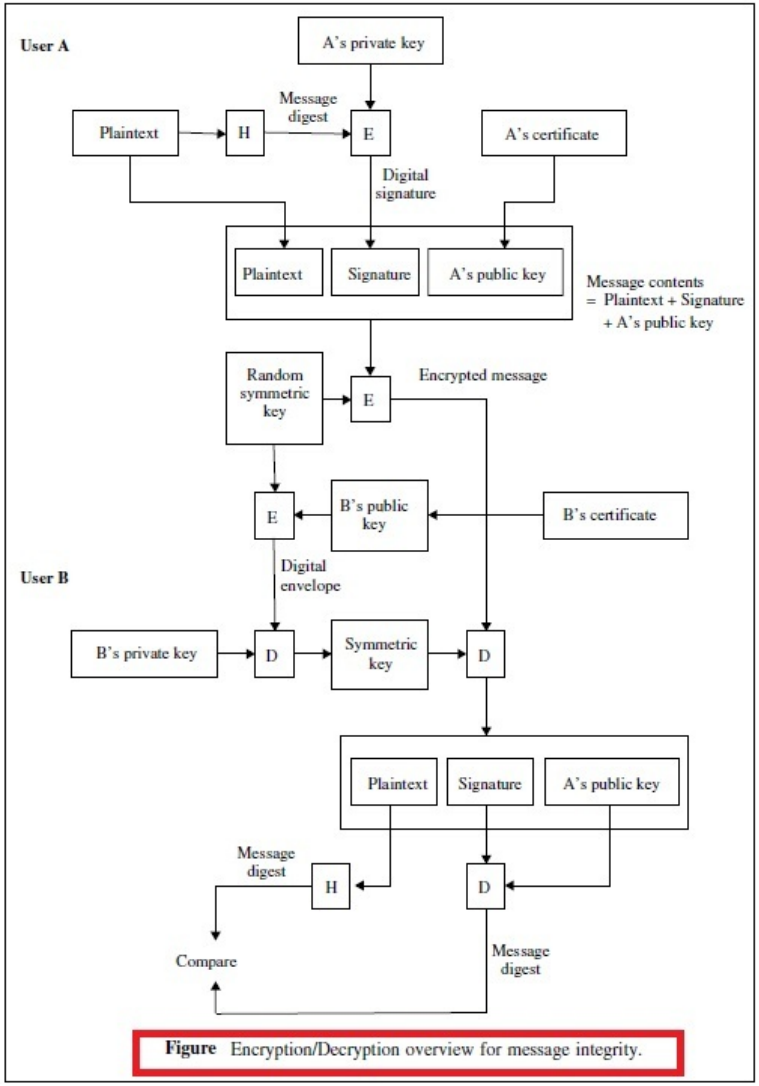


Figure Encryption/Decryption overview for message integrity.

SET for E-commerce Transactions(Contd..)

Payment Processing

- Cardholder Registration:Registration request/response processes, Registration form process, Certificate request/response processes,
- Merchant Registration : Registration form process, Certificate request/create process
- Purchase Request: Initiate request, Initiate response, Purchase request, Purchase response.
- Payment Authorisation : Authorisation request, Authorisation response
- Payment Capture: Capture request, Capture response.

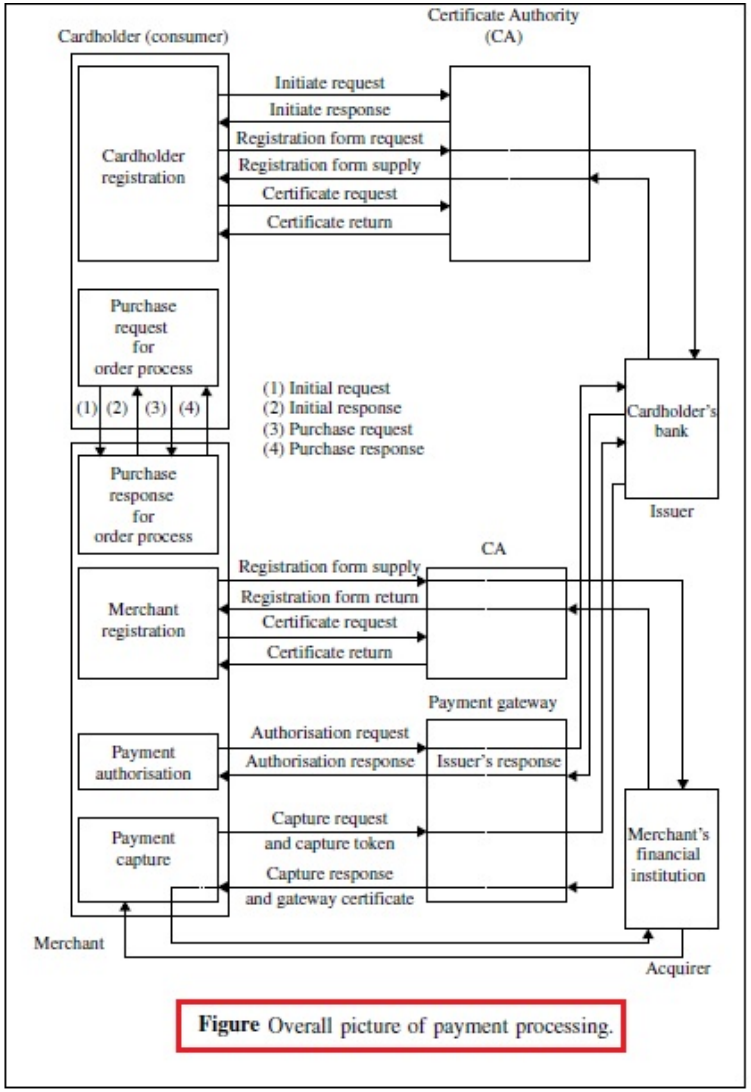


Figure Overall picture of payment processing.

Assessment

- What is the purpose of a Firewall?
- What are the commonly used Firewall types?
- Explain the operation of the packet-filter firewall.
- Explain the operation of the Application Gateway Firewall.
- What is NAT? How it improves network security?