## WEB SECURITY

Is the process of securing confidential data stored online from unauthorized and modification.

Also known as " cyber security" involves protecting website or web application by detecting, preventing & responding to attacks.

## The Aim Of Web Security Is To Identify:-

Critical assets of organization.

Genuine users who may access data.

Level of access provide to each user.

Various vulnerabilities that may exist in application.

Risk analysis on data exposure.

Website relating to Banking, E-commerce, Social Networking, Web mail etc.

## PRINCIPLES OF SECURITY

Confidentiality

Integrity

Availability

Nonrepudiation

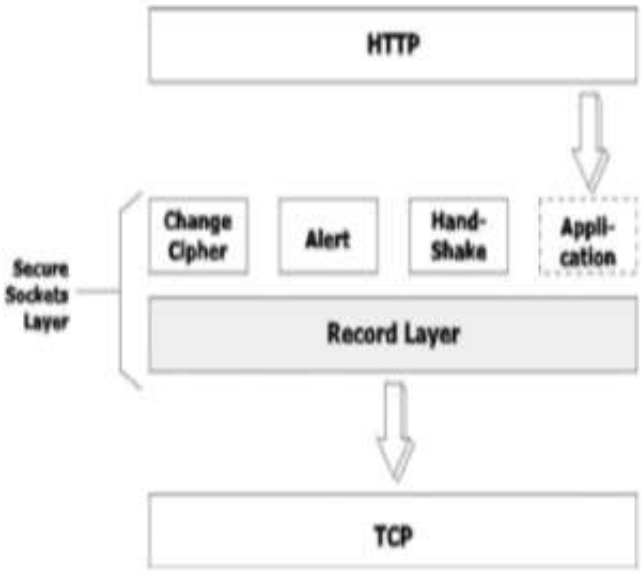
# Introduction to SSL

- The overall goal of the **Secure Sockets Layer (SSL)** protocol is to provide privacy and reliability between two communicating applications.
  - SSL was developed by Netscape.
  - Evolved through an unreleased v1 (1994), flawed-but-useful v2
  - The current version of the SSL protocol is Version 3 (V3),specification released March 1996.
  - Standard TLS1.0 (Jan 1999) is just SSL3.0 with minor tweaks,hence Version field is 3.1

- Defined in RFC2246,http://www.ietf.org/rfc/rfc2246.txt
- Open-source implementation at http://www.openssl.org/
- Protocol allows client/server applications to communicate in a way designed to prevent eavesdropping, tampering, or message forgery.

# SSL Record Layer Protocol

- SSL uses its **Record Layer Protocol** to encapsulate all messages.
- It provides a common format to frame the following message types:
  - Alert
  - ChangeCipherSpec
  - Handshake
  - Application protocol Messages

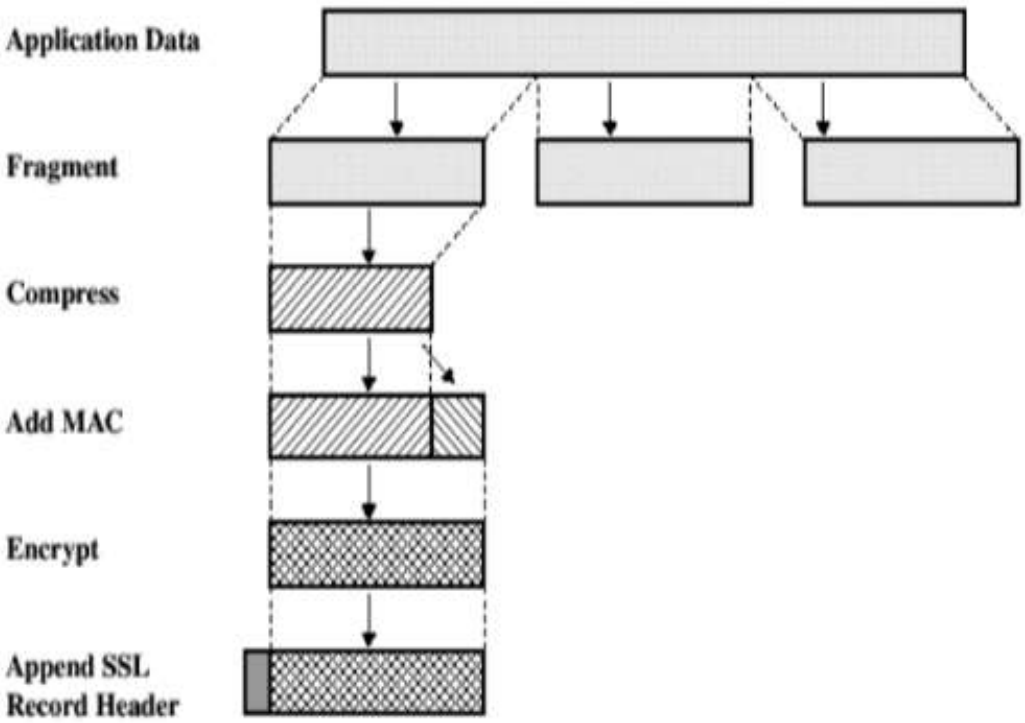



# SSL Record Layer Protocol

- The Record Layer formatting consists of 5 bytes that precede other protocol message.
  - If message integrity is active, a message authentication code is placed at the end of the message.
  - If encryption is active, this layer is also responsible for the encryption process.

# SSL Record Layer Protocol

- The Record Layer Protocol takes an application message and performs the following operations:
  - Fragments the data into manageable blocks.
  - Optionally, compresses the data.
    - Default is no compression.



## SSL Record Layer Protocol

- Adds a message authentication code (MAC).
- Encrypts the data plus MAC using symmetric encryption.
- Prepends a header.
- Transmits the unit in a TCP segment.

## SSL Record Layer Protocol

- Some values:
- **Fragment size:** (no more than) 214 bytes, or 16,384 bytes.
- **Compression:** This operation may not increase content Length by more than 1024 bytes.
  - However, it should shrink it!

## SSL Record Layer Protocol

- Message authentication code is calculated over the data using a shared secret key as follows:

  hash(MAC_write_secret || pad_2 ||
  hash(MAC_write_secret || pad_1 || seq_num ||
  SSLCompressed.type || SSLCompressed.length ||
  SSLCompressed.fragment) )

## SSL Record Layer Protocol

where:
|| represents concatenation
MAC_write_secret represents the shared secret key.
hash represents the cryptographic hash algorithm (either MD5 or SHA-1).
pad_1 represents the byte 0x36 repeated 48 times (384 bits) for MD5 and 40 times for SHA-1.
pad_2 represents the byte 0x5C repeated 48 times for MD5 and 40 times for SHA-1.

# SSL Record Layer Protocol

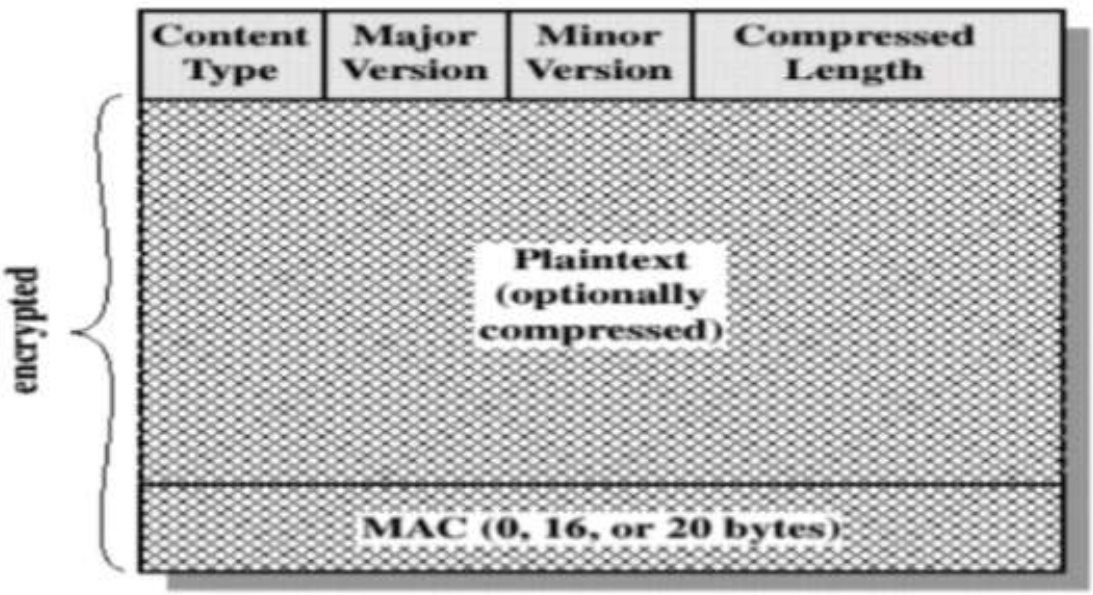
**seq_num** represents the sequence number for this fragment.
**SSLCompressed.type** represents the higher level protocol used to process this message.
**SSLCompressed.length** represents the length of the compressed fragment.
**SSLCompressed.fragment** represents the compressed (or plaintext) fragment.

# SSL Record Layer Protocol

- **Encryption:** After encrypting the plaintext (or , compressed plaintext) message plus the MAC, The overall message size should not be more than 214 + 2048 bytes
- Valid encryption algorithms:
  - IDEA, DES, DES-40,3DES, RC2-40,Fortezza
  - RC4-40 & RC4-128

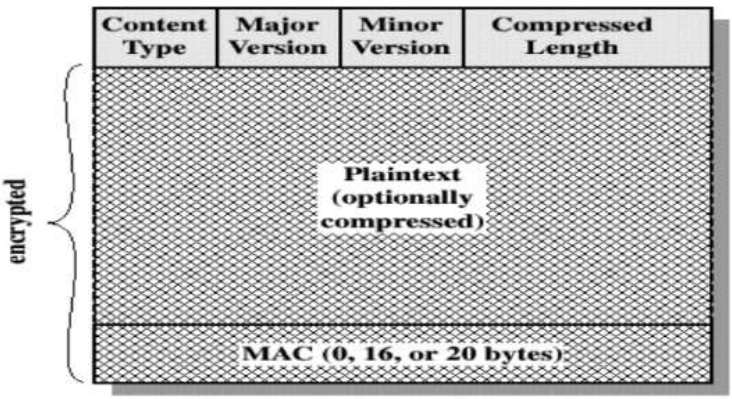
# SSL Record Layer Protocol: Header

- The pre-pended header consists of the following fields:
  - **Content Type:** An 8-bit field to define the higher layer protocol encapsulated.
  - The content types defined are:
    - 20: ChangeCipherSpec
    - 21: Alert
    - 22: Handshake
    - 23: Application



## SSL Record Layer Protocol: Header

- The pre-pended header consists of the following fields:
  - **Content Type:** An 8-bit field to define the higher layer protocol encapsulated.
  - The content types defined are:
    - 20: ChangeCipherSpec
    - 21: Alert
    - 22: Handshake
    - 23: Application



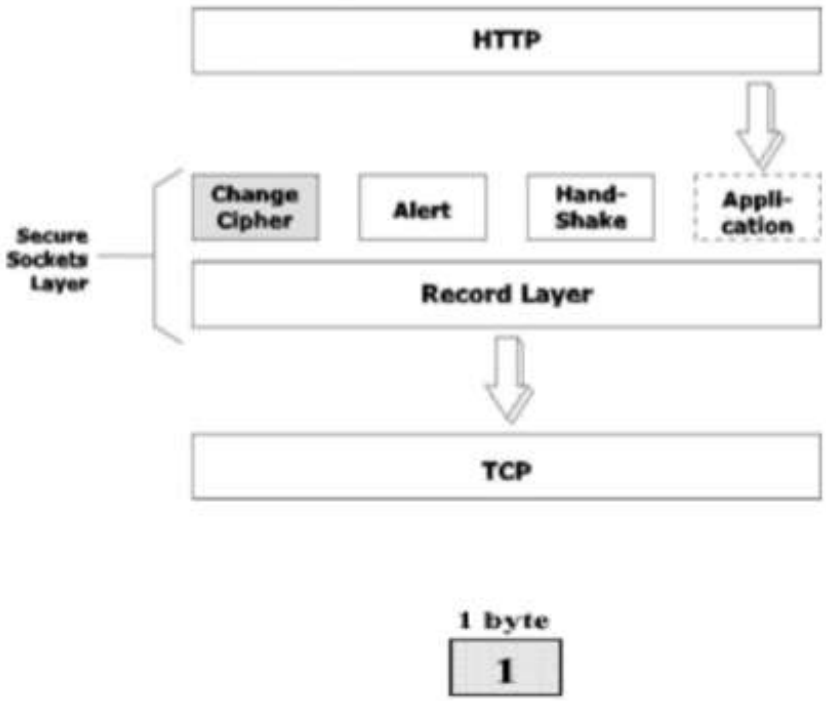

## SSL Record Layer Protocol: Header

## SSL Record Layer Protocol: Header

- **Major Version:** An 8-bit field which indicates the major version of SSL is in use (e.g., 3).
- **Minor Version:** An 8-bit field which indicates the minor version of SSL is in use (e.g., 0).
- **Compressed Length:** An 16-bit field which indicates the length of the compressed (plaintext) fragment.

## SSL Change Cipher Spec Protocol

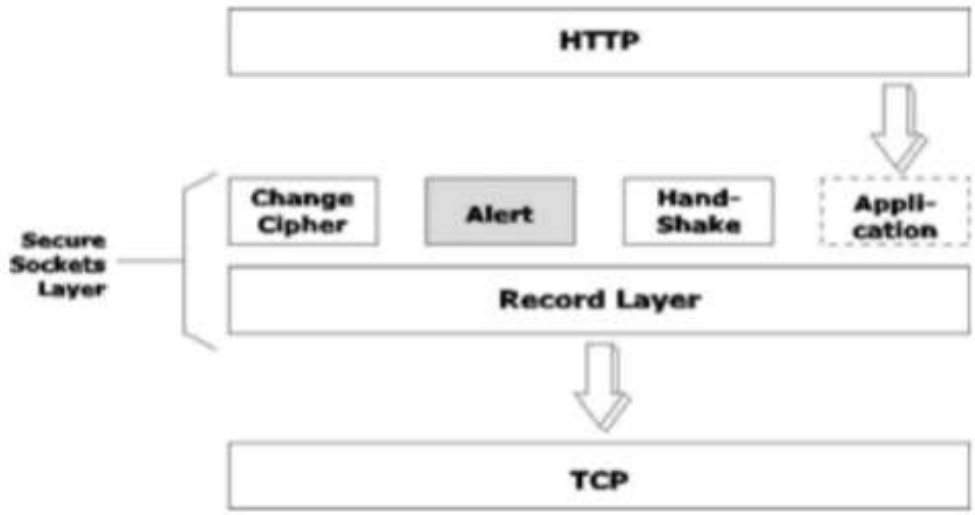
- The **ChangeCipherSpec Protocol** is simplest possible protocol since it has only one message.
  - It consists of a single byte with a value of 1.
- This message causes a pending state to be copied into the current state which updates the cipher suite to be used on the connection.

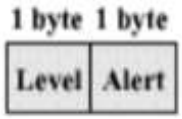





## SSL Alert Protocol

- The **Alert Protocol** is used to signal an error, or caution,condition to the other party in the communication.
- Two bytes
- The first byte takes either of the following two values :
  - "1" indicates a warning.
  - "2" indicates a fatal error.
- Fatal errors terminate the connection.






## SSL Alert Protocol

Warning or fatal (*)

close_notify(0),

- unexpected_message(10),

bad_record_mac(20),
decryption_failed(21),
record_overflow(22),

- decompression_failure(30),
- handshake_failure(40),

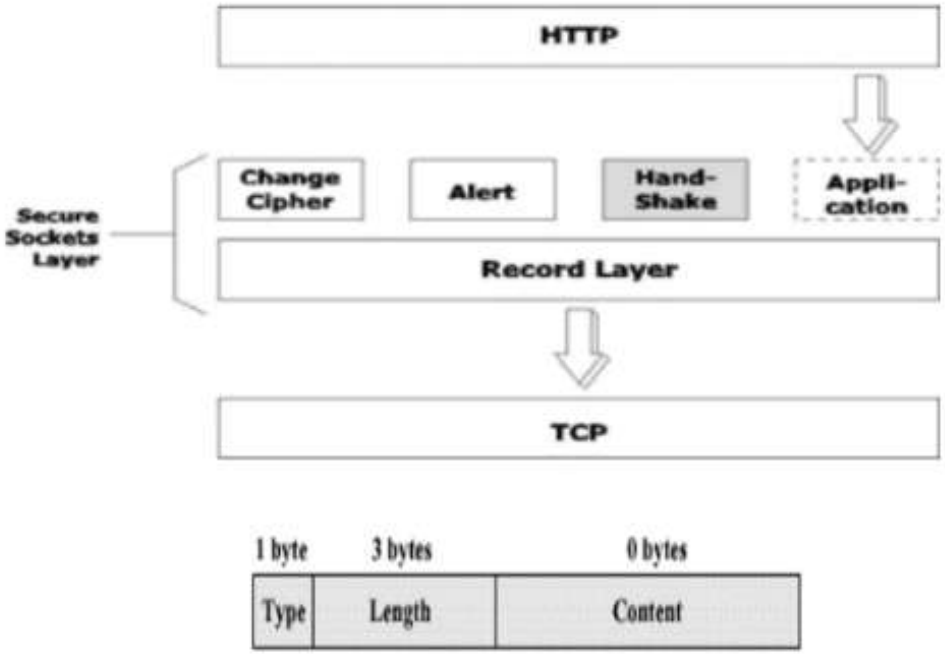
bad_certificate(42),
unsupported_certificate(43),
certificate_revoked(44),
certificate_expired(45),
certificate_unknown(46),

- **Illegal_parameter(47),**
  **unknown_ca(48),**
  **access_denied(49),**
  **decode_error(50),**
  **decrypt_error(51),**
  **export_restriction(60),**
  **protocol_version(70),**
  **insufficient_security(71),**
  **internal_error(80),**
  **user_canceled(90),**
  **no_renegotiation(100)**



## SSL Handshake Protocol

- The most complex part of SSL is the **Handshake Protocol.**
- provides means for client and server to:
  - Authenticate each other.
  - Negotiate an encryption and MAC algorithm.
  - Negotiate the secret key to be used.
- This protocol consists of a series of messages.
  Each message consists of three fields:
  - **Type:** A 8-bit field indicating the type of message (1 of 10).
  - **Length:** A 3-byte field-length field.
  - **Content:** >=0-byte field for message parameters.





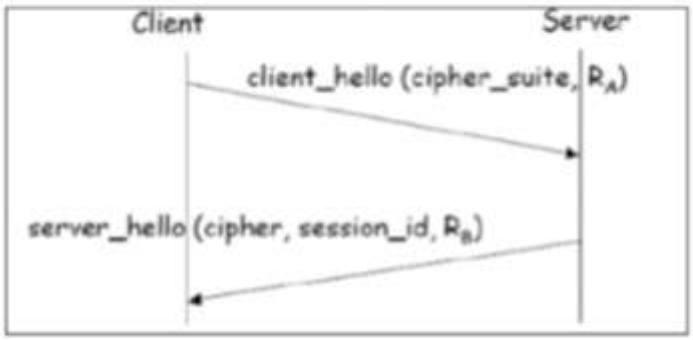

## Message Exchange

- In SSL, the message exchange process is used to:
  - Authenticate the server.
  - Authenticate the client.
  - Select a cipher.
  - Exchange a key.
  - Transfer data.
- All messages during handshaking and after, are sent over the SSL Record Protocol layer.

## SSL Handshake Protocol

**Phase 1** – Establishing security capabilities.

- This phase comprises of exchange of two messages – *Client_hello* and *Server_hello*.

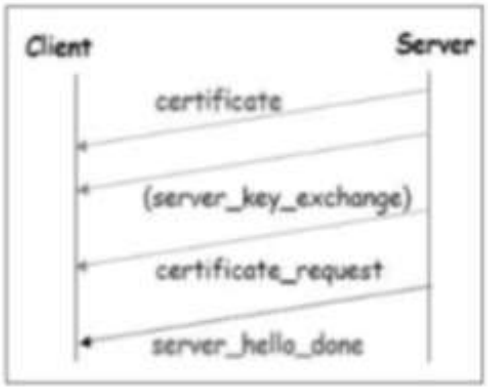





- *Client_hello* contains of list of cryptographic algorithms supported*C* by the client, in decreasing order of preference.
- *Server_hello* contains the selected Cipher Specification (CipherSpec) and a new *session_id*.
- The CipherSpec contains fields like –
  - Cipher Algorithm (DES, 3DES, RC2, and RC4)
  - MAC Algorithm (based on MD5, SHA-1)
  - Public-key algorithm (RSA)
  - Both messages have "nonce" to prevent replay attack.

## Phase 2 – Server authentication and key exchange.

- Server sends certificate. Client software comes configured with public keys of various "trusted" organizations (CAs) to check certificate.
- Server sends chosen cipher suite.




- Server may request client certificate.Usually it is not done.
- Server indicates end of *Server_hello*.



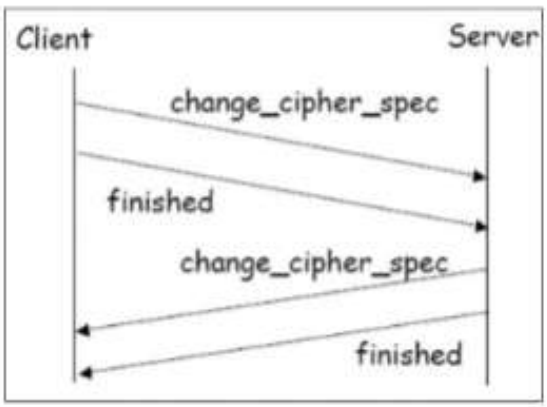
## Phase 3 - Client authentication and key exchange.

- Client sends certificate, only if requested by the server.
- It also sends the Pre-master Secret (PMS) encrypted with the server's public key.


- Client also sends *Certificate_verify* message if certificate is sent by him to prove he has the private key associated with this certificate. Basically, the client signs a hash of the previous messages.

## Phase 4 – Finish.

- Client and server send *Change_cipher_spec* messages to each other to cause the pending cipher be copied into the current state.




- From now on, all data is encrypted and integrity protected.
- Message "Finished" from each end verifies that the key exchange and authentication processes were successful.

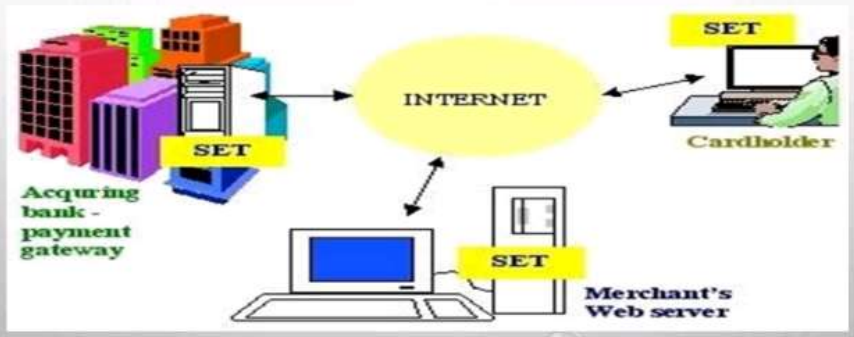
# CONTENT

- Introduction for Secure Electronic Transaction(SET)
- Requirement for SET
- SET Protocols
- Key Features of SET
- Participate of SET
- SET Components
- SET Transaction

## Secure electronic transaction SET:-

- ✓ Secure electronic transaction is an open source encryption and specification.
- ✓ It is designed for protecting credit card transaction on the internet.
- ✓ Companies involved:- MasterCard, Visa , Microsoft ,Netscape , Cyber Cash.
- ✓ Remember that a secure electronic transaction is not a payment system , it is a set of security protocols and format that ensure that using online payment transaction on the internet is secure.
- ✓ Secure electronic transaction is also called as SET.
- ✓ SET provide a secure environment for all the parties that are involved in the e-commerce transaction.
- ✓ It also ensures confidentiality.it provides trust by the use of **X.509v3** through digital certificate.

## Secure Electronic Transaction:-




## SET Requirements:-

- Provide confidentiality of payment and ordering information.
- Ensure the integrity of all transmitted data.
- Provide authentication that a cardholder is a legitimate user of a credit card account.
- Provide authentication that a merchant can accept credit card transaction through its relationship with a financial institution.
- It has to keep the PI(Payment Information) formation)confidential by appropriate encryption

## SET Requirements:-

- Provide confidentiality of payment and ordering information.
- Ensure the integrity of all transmitted data.
- Provide authentication that a cardholder is a legitimate user of a credit card account.
- Provide authentication that a merchant can accept credit card transaction through its relationship with a financial institution.
- It has to keep the PI(Payment Information) and OI(Order Information)confidential by appropriate encryption.
- It has to be resistive against message modifications i.e. no change should be allowed in the content being transmitted.
- SET also need to provide interoperability and make use of best security mechanisms.

## SET protocols:-

- **Confidentiality –** All messages are encrypted.
- **Trust –** All parties must have digital certificates.
- **Privacy –** Information made available only when and where necessary.
- **Developed –** Developed by visa and master card.
- **Design –** Designed to protect credit card transaction.

## key Factures:-

- **Confidentiality of information** :- Cardholder account and payment information is secured as it travels occurs the network . An interesting and important feature of SET is that it prevents the merchant from learning the cardholder's credit card numbers this is only provided to the issuing bank conventional encryption by DES is used to provide confidentiality.
- **Integrity of data** :- Payment information sent from cardholders to merchants included order information, personal data and payment instructions .SET guarantees that these message contents are not altered in transit . RSA digital signatures , using SHA-1 hash codes , provide message integrity . Certain message are also protected by HMAC using SHA-1.
- **Cardholder account authentication** :- SET enable merchants to verify that a cardholder is a legitimate user of a valid card account number . SET uses X.509v3 digital certificates with RSA signatures for this purpose.
- **Merchant authentication** :-SET enables cardholder to verify that a merchant has a relationship with a financial institution allowing it to accept payment cards . SET uses X.509v3 digital certificates with RSA signatures for this purpose.

## Participants of SET :-

A SET system includes the following participants:-

- **Cardholder**
- **Merchant**
- **Issuer**
- **Acquire**
- **Payment gateway**

message are also protected by HMAC using SHA-1.

❖ **Cardholder account authentication** :- SET enable merchants to verify that a cardholder is a legitimate user of a valid card account number . SET uses X.509v3 digital certificates with RSA signatures for this purpose.

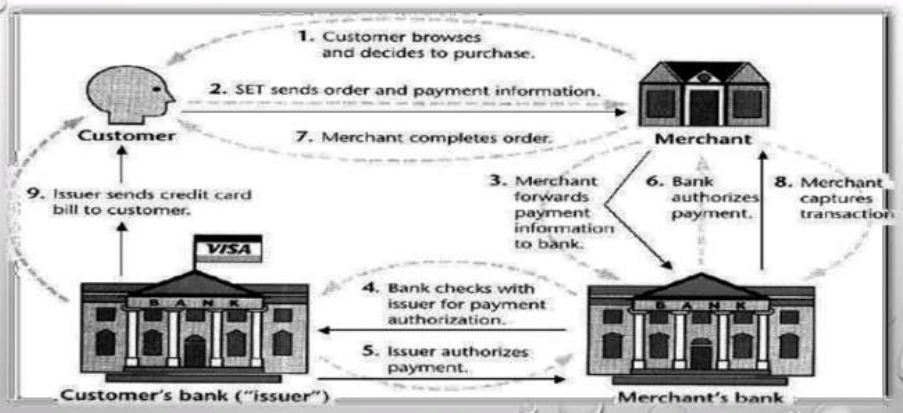
❖ **Merchant authentication** :-SET enables cardholder to verify that a merchant has a relationship with a financial institution allowing it to accept payment cards . SET uses X.509v3 digital certificates with RSA signatures for this purpose.

## Participants of SET :-

A SET system includes the following participants:-

- Cardholder
- Merchant
- Issuer
- Acquire
- Payment gateway
- Certificate authority

## SET COMPONENTS:-



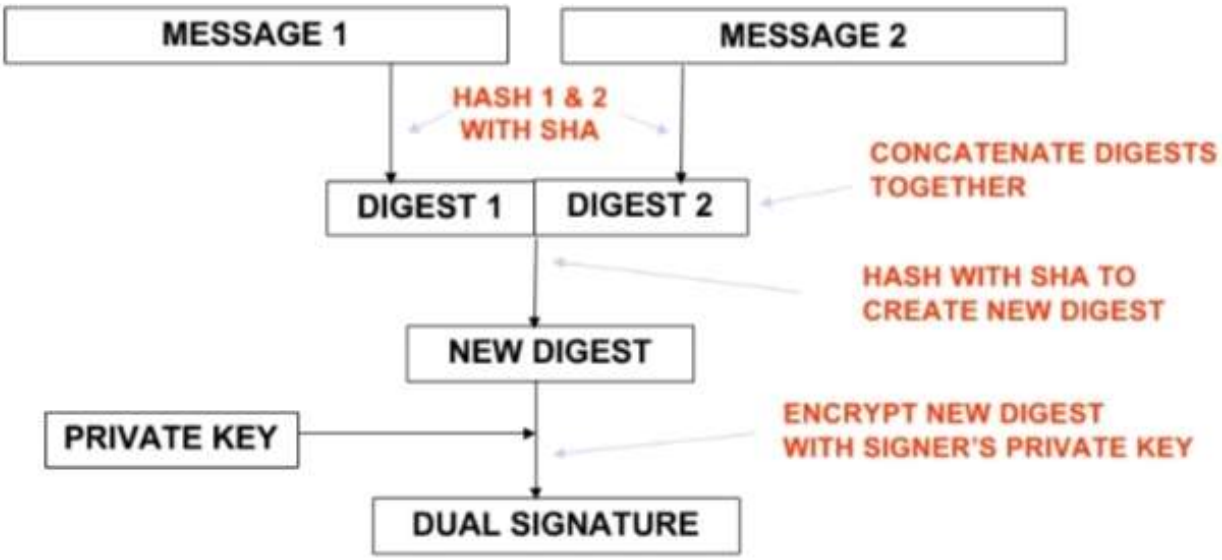

## SET TRANSACTION:-

Both cardholders and merchants must register with the CA (certificate authority) first ,before they can buy or sell on the internet . Once registration is done , cardholder and merchant can start to do transactions which involve nine basic steps in this protocol , which is simplified.

- Customer browses the website and decides on what to purchase
- Customer sends the order and payment information , which includes two parts is one message:
- **Purchase order - this** part is for merchant.
- **Card information - this** part is for merchant's bank only.
- Merchant forwards card information to their bank.
- Merchant's bank checks with the issuer for payment authorization.
- Issuer sends authorization to the merchant's bank.
- Merchant's bank sends authorization to the merchant.
- Merchant completes the order and sends confirmation to the customer.
- Merchant captures the transaction from their bank.
- Issuer prints credit card bill(invoice) to the customer.

# Dual Signatures

- Links two messages securely but allows only one party to rea d each.

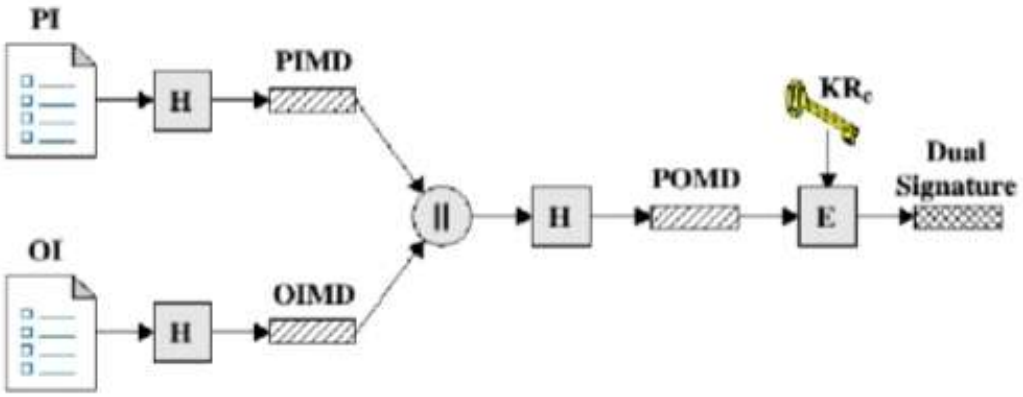





# Dual Signature for SET

- Concept: Link Two Messages Intended for Two Differ ent Receivers:
  - Order Information (OI): Customer to Merchant
  - Payment Information (PI): Customer to Bank
- Goal: Limit Information to A "Need-to-Know" Basis:
  - Merchant does not need credit card number.
  - Bank does not need details of customer order.
  - Afford the customer extra protection in terms of p rivacy by keeping these items separate.
- This link is needed to prove that payment is intended f or this order and not some other one.

# Dual Signature Operation




- The operation for dual signature is as follows:
  - Take the hash (SHA-1) of the payment and order information.
  - These two hash values are concatenated [H(PI) || H(OI)] and t hen the result is hashed.
  - **Customer encrypts the final hash with a private key creating th e dual signature.**

$$DS = E_{KRC} [ H(H(PI) || H(OI)) ]$$



# DS Verification by Merchant

- The merchant has the public key of the customer obtai ned from the customer's certificate.
- Now, the merchant can compute two values:

  $H(PIMD || H(OI))$

  $D_{KUC}[DS]$
- Should be equal!

# DS Verification by Bank

- The bank is in possession of DS, PI, the message digest for OI (OIMD), and the customer's public key, then the bank ca n compute the following:

  $H(H(PI) \,||\, OIMD)$

  $D_{KUC}$ [ DS ]



# SET Supported Transactions

- card holder registration
- merchant registration
- purchase request
- payment authorization
- payment capture
- certificate query
- purchase inquiry
- **purchase notification**
- **sale transaction**
- **authorization reversal**
- **capture reversal**
- **credit reversal**

## Purchase Request

- Browsing, Selecting, and Ordering is Done
- Purchasing Involves 4 Messages:
  - Initiate Request
  - Initiate Response
  - Purchase Request
  - Purchase Response



## Payment Process

- The payment process is broken down into two steps:
  - Payment authorization
  - Payment capture

# System security

- The Security Problem
- Program Threats
- System and Network Threats
- Cryptography as a Security Tool
- User Authentication
- Implementing Security Defenses
- Firewalling to Protect Systems and Networks
- Computer-Security Classifications

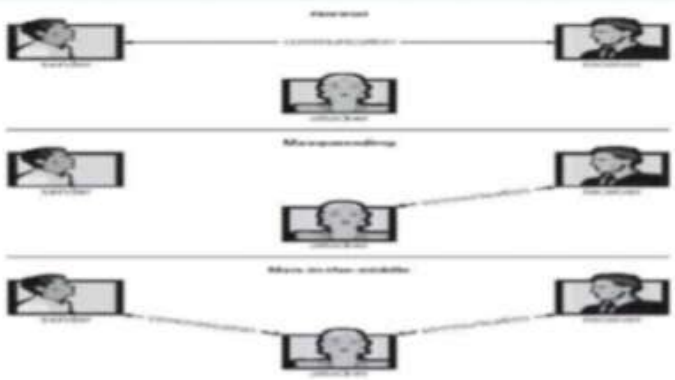
# Security problems

- Security must consider external environment of the system, and protect the system resources
- Intruders (crackers) attempt to breach security
- **Threat** is potential security violation
- **Attack** is attempt to breach security
- Attack can be accidental or malicious
- Easier to protect against accidental than malicious misuse

# Security violations

- Categories
  - **Breach of confidentiality**
  - **Breach of integrity**
  - **Breach of availability**
  - **Theft of service**
  - **Denial of service**
- Methods
  - **Masquerading (breach authentication)**
  - **Replay attack**
    - **Message modification**
  - **Man-in-the-middle attack**
  - **Session hijacking**

# Standard security Attacks



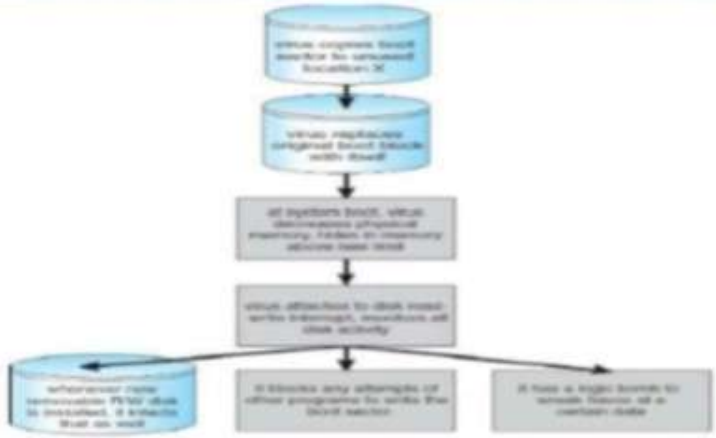
# Standard measure levels

- Security must occur at four levels to be effective:
  - Physical
  - Human
    - Avoid **social engineering, phishing, dumpster diving**
  - Operating System
  - Network
- Security is as week as the weakest chain

# Program Threats

- Trojan Horse
  - Code segment that misuses its environment
  - Exploits mechanisms for allowing programs written by users to be executed by other users
  - **Spyware, pop-up browser windows, covert channels**
- Trap Door
  - Specific user identifier or password that circumvents normal security procedures
  - Could be included in a compiler
- Logic Bomb
  - Program that initiates a security incident under certain circumstances
- Stack and Buffer Overflow
  - Exploits a bug in a program (overflow either the stack or memory buffers)

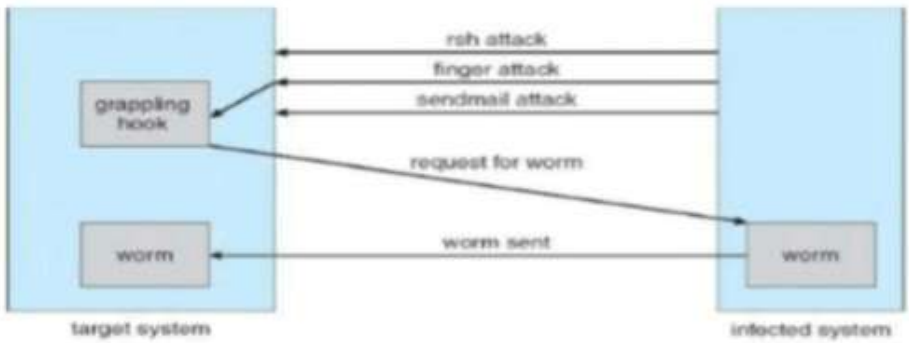
# A Boot-sector computer virus



# System and Network Threats

- Worms – use **spawn** mechanism; standalone program
- Internet worm
  - Exploited UNIX networking features (remote access) and bugs in *finger* and *sendmail* programs
  - **Grappling hook** program uploaded main worm program
- Port scanning
  - Automated attempt to connect to a range of ports on one or a range of IP addresses
- Denial of Service
  - Overload the targeted computer preventing it from doing any useful work
  - Distributed denial-of-service (**DDOS**) come from multiple sites at once

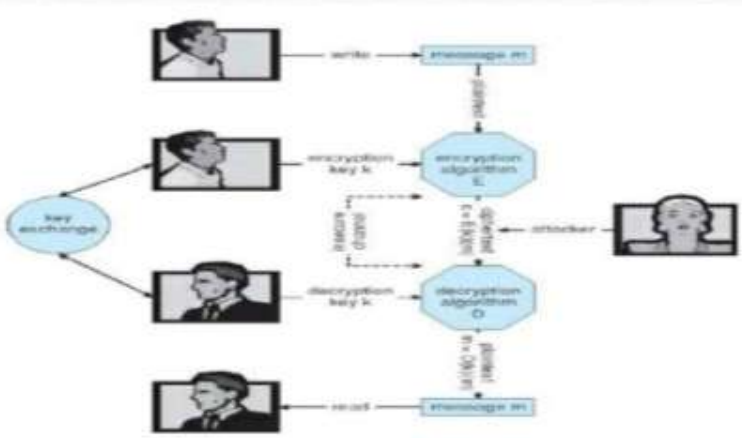
# The Morris Internet Worm



# Cryptography as a Security Tool

- Broadest security tool available
  - Source and destination of messages cannot be trusted without cryptography
  - Means to constrain potential senders (*sources*) and / or receivers (*destinations*) of *messages*
- Based on secrets (**keys**)

# Secure communication over insecure medium



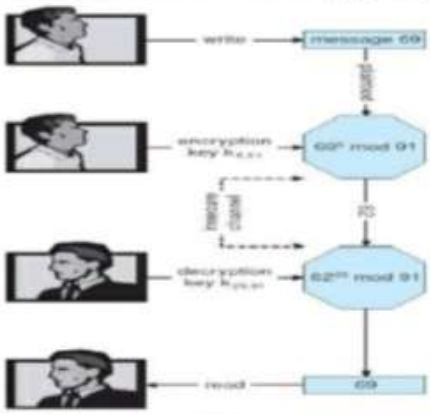
# Encryption

- Encryption algorithm consists of
  - Set of *K* keys
  - Set of *M* Messages
  - Set of *C* ciphertexts (encrypted messages)
  - A function $E : K \rightarrow (M \rightarrow C)$. That is, for each $k \in K$, $E(k)$ is a function for generating ciphertexts from messages.
    - Both $E$ and $E(k)$ for any $k$ should be efficiently computable functions.
  - A function $D : K \rightarrow (C \rightarrow M)$. That is, for each $k \in K$, $D(k)$ is a function for generating messages from ciphertexts.
    - Both $D$ and $D(k)$ for any $k$ should be efficiently computable functions.
- An encryption algorithm must provide this essential property: Given a ciphertext $c \in C$, a computer can compute $m$ such that $E(k)(m) = c$ only if it possesses $D(k)$.
  - Thus, a computer holding $D(k)$ can decrypt ciphertexts to the plaintexts used to produce them, but a computer not holding $D(k)$ cannot decrypt ciphertexts.
  - Since ciphertexts are generally exposed (for example, sent on the network), it is important that it be infeasible to derive $D(k)$ from the ciphertexts

# Symmetric encryption

- Same key used to encrypt and decrypt
  - $E(k)$ can be derived from $D(k)$, and vice versa
- DES is most commonly used symmetric block-encryption algorithm (created by US Govt)
  - Encrypts a block of data at a time
- Triple-DES considered more secure
- Advanced Encryption Standard (**AES**), **twofish** up and coming
- RC4 is most common symmetric stream cipher, but known to have vulnerabilities
  - Encrypts/decrypts a stream of bytes (i.e wireless transmission)
  - Key is a input to psuedo-random-bit generator
    - Generates an infinite **keystream**

# Encryption and Decryption using RSA Asymmetric Cryptography



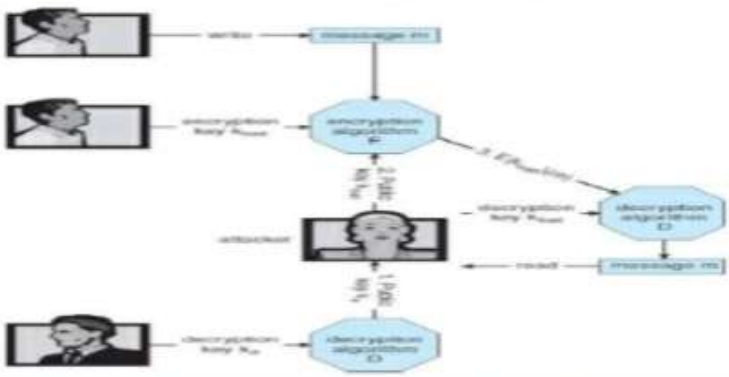

# Cryptography (cont... )

- Note symmetric cryptography based on transformations, asymmetric based on mathematical functions
  - Asymmetric much more compute intensive
  - Typically not used for bulk data encryption

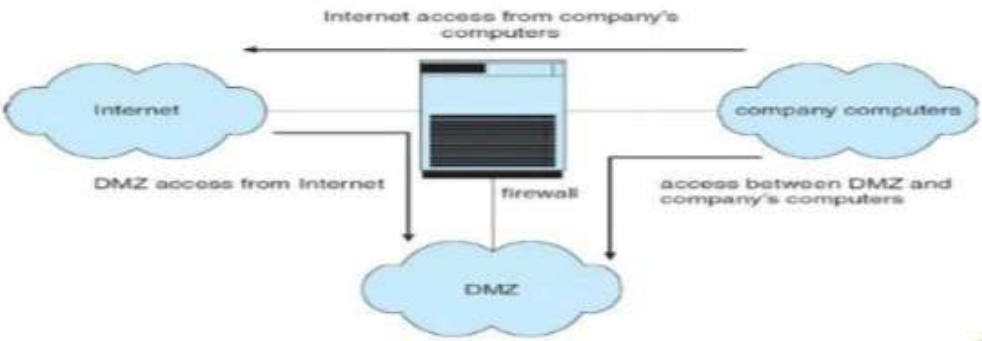
# Key distribution

- Delivery of symmetric key is huge challenge
  - Sometimes done **out-of-band**
- Asymmetric keys can proliferate – stored on **key ring**
  - Even asymmetric key distribution needs care – man-in-the-middle attack

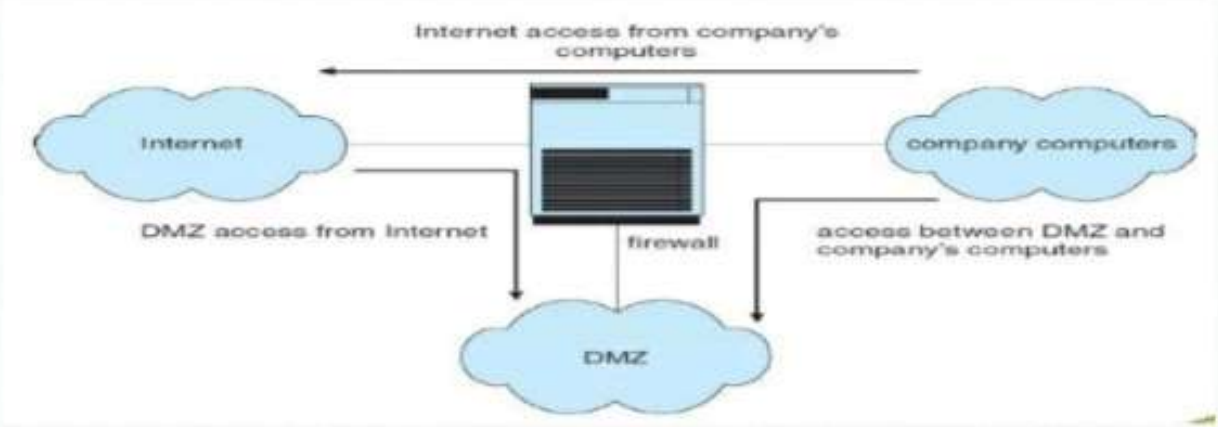
# Man-in-the middle attack on asymmetric cryptography



# Network security through domain separation via firewall



# Network security through domain separation via firewall




# Computer security classification

- U.S. Department of Defense outlines four divisions of computer security: **A**, **B**, **C**, and **D**.
- **D** – Minimal security.
- **C** – Provides discretionary protection through auditing. Divided into **C1** and **C2**. **C1** identifies cooperating users with the same level of protection. **C2** allows user-level access control.
- **B** – All the properties of **C**, however each object may have unique sensitivity labels. Divided into **B1**, **B2**, and **B3**.
- **A** – Uses formal design and verification techniques to ensure security.

# INTRUSION TECHNIQUES

- Techniques for guessing passwords:
  - Try default passwords.
  - Try all short words, 1 to 3 characters long.
  - Try all the words in an electronic
  - Collect information about the user's hobbies, names, birthday, etc.
  - Try user's phone number, social security number, street address, etc.
  - Try all license plate numbers (MUP103).
  - Use a Trojan horse
  - Tap the line between a remote user and the host system.

Prevention: Enforce good password selection (Ij4Gf4Se%f#)

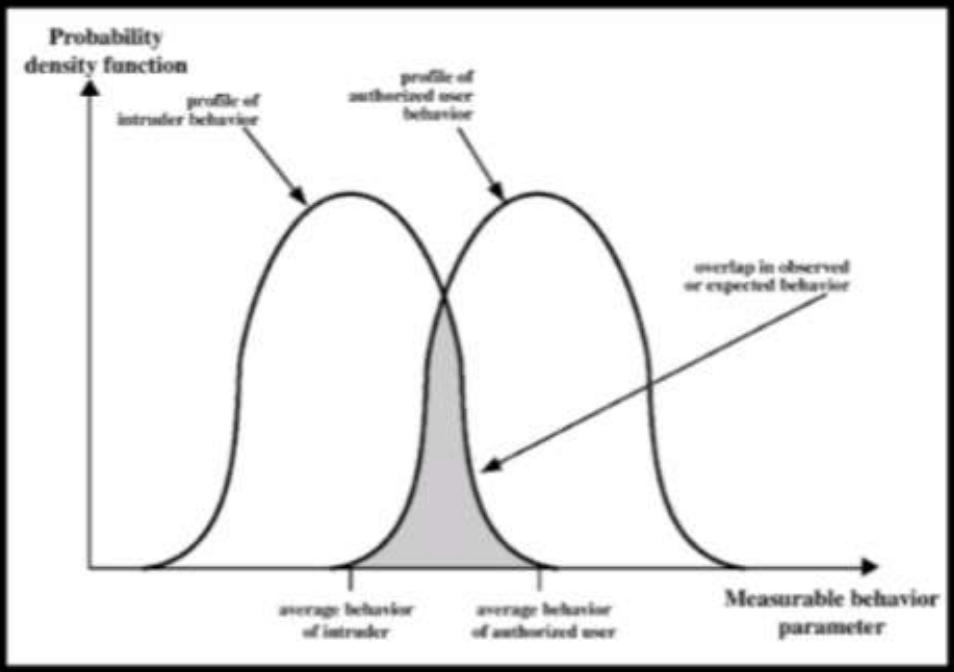




# PASSWORD SELECTING STRATEGIES

- User ducation
- Computer-generated passwords
- Reactive password checking
- Proactive password checking

# PROFILES OF BEHAVIOR OF INTRUDERS AND AUTHORIZED USERS




Henric Johnson



# INTRUSION DETECTION

- Signature Based Detection:

It can easily detect the attacks whose pattern (signature) already exists in system but it is difficult to detect the new malware attacks as their pattern (signature) is not known.

2. Anomaly detection

It was introduced to detect the unknown malware attacks. In it there is use of machine learning to create a trustful activity model and anything coming is compared with that model.

# MEASURES USED FOR INTRUSION DETECTION



- Login frequency by day and time.
- Frequency of login at different locations.
- Time since last login.
- Password failures at login.
- Execution frequency.
- Execution denials.
- Read, write, create, delete frequency.
- Failure count for read, write, create and delete.

# Definitions

- Virus - code that copies itself into other programs.
- A "Bacteria" replicates until it fills all disk space, or CPU cycles.
- Payload - harmful things the malicious program does, after it has had time to spread.
- Worm - a program that replicates itself across the network (usually riding on email messages or attached documents (e.g., macro viruses).



# Definitions

- Trojan Horse - instructions in an otherwise good program that cause bad things to happen (sending your data or password to an attacker over the net).
- Logic Bomb - malicious code that activates on an event (e.g., date).
- Trap Door (or Back Door) - undocumented entry point written into code for debugging that can allow unwanted users.
- Easter Egg - extraneous code that does something "cool." A way for programmers to show that they control the product.

# Types of Viruses

- **Parasitic Virus** - attaches itself to executable files as part of their code. Runs whenever the host program runs.
- **Memory-resident Virus** - Lodges in main memory as part of the residual operating system.
- **Boot Sector Virus** - infects the boot sector of a disk, and spreads when the operating system boots up (original DOS viruses).
- **Stealth Virus** - explicitly designed to hide from Virus Scanning programs.
- **Polymorphic Virus** - mutates with every new host to prevent signature detection.

## What is Firewalls ?

- a **choke point** of control and monitoring
- interconnects networks with differing trust
- imposes restrictions on network services
  – only authorized traffic is allowed
- auditing and controlling access
  – can implement alarms for abnormal behavior
- provide NAT & usage monitoring
- implement VPNs using IPSec
- must be immune to penetration

## Hardware Vs. Software Firewalls

Hardware Firewalls

- Protect an entire network.
- Implemented on the router level.
- Usually more expensive,harder to configure.

Software Firewalls

- Protect a single computer.
- Usually less expensive, easier to configure.

## Firewalls Rules

- **Allow-** traffic that flows automatically because it has been it demeed.
- **Block-** traffic that is blocked because it has been demeed dangerous to your computer.
- **Ask -** ask the user whether or not the traffic is allowed to pass through.

## Firewalls Rules

- **Allow-** traffic that flows automatically because it has been it demeed.
- **Block-** traffic that is blocked because it has been demeed dangerous to your computer.
- **Ask -** ask the user whether or not the traffic is allowed to pass through.

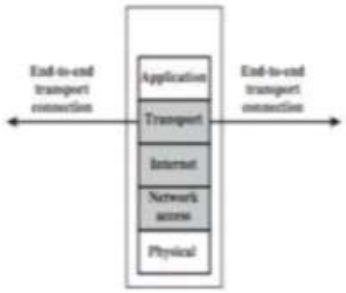
## Firewalls Limitations

- cannot protect from attacks bypassing it
  - eg sneaker net, utility modems, trusted organisations, trusted services (eg SSL/SSH)
- cannot protect against internal threats
  - eg disgruntled or colluding employees
- cannot protect against access via WLAN
  - if improperly secured against external use
- cannot protect against malware imported via laptop, PDA, storage infected outside

# Types of firewalls

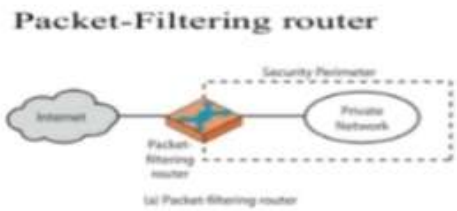
- Packet filtering firewall
- Application proxy firewall
- Circuit-level proxy firewall

# Packet Filtering Firewall




# Packet Filtering Firewall

- A Packet filtering firewall applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet.
- Filtering rules are based on information contained in a network packet.
- Source IP address, destination IP address ,port number etc..



# Packet filtering firewall

- Two default polices are three to take default action determine whether to forward or discard the packet.

  Default= discard

  Default =forward

- Some possible attacks on firewall:

  IP address spoofing

  Source routing attacks

  Tiny fragment attacks.

# Packet filtering firewall

- **Advantage:**

  Cost

  Low resource usage

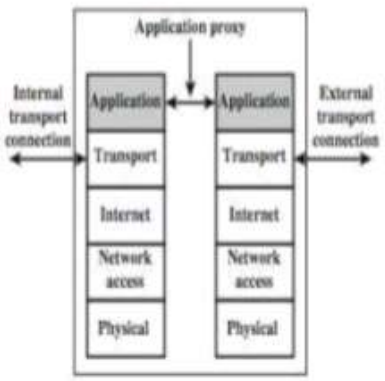
  Best suitable for smaller network.

- **Disadvantage:**

  Can work only on the network layer

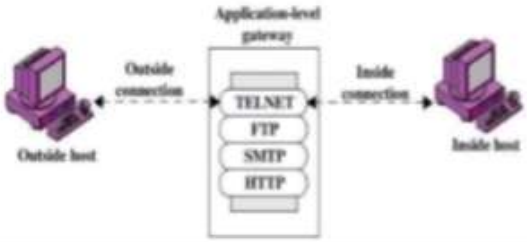
  Do not support complex rule based support.

# Application Proxy Firewall



# Application Proxy Firewall

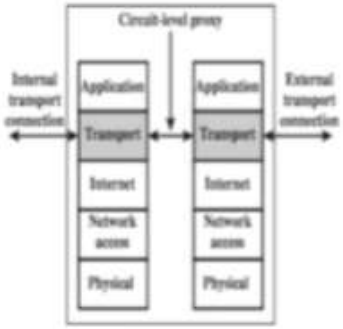
- An application-level gateway , also called on application proxy , acts as relay of application-level traffic.
- User request service from proxy.
- Proxy validates request as legal.
- Then actions request and returns result to user.
- Can log/audit traffic at application level.




# Application Proxy Firewall

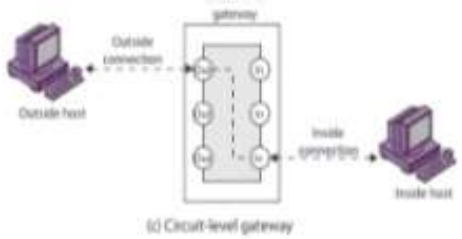
- **Advantage:**
  - Most secure than packet filtering firewalls.
  - Easy to log and audit incoming traffic.
- **Disadvantage:**
  - Additional processing overhead on each connections.

# Circuit -Level Firewall



# Circuit-Level Firewall

- This can be a stand-alone system
- It does not permit an end-to -end TCP connection ;rather ,the gateway sets two TCP connections.
- A typical use of the circuit-level gateway is a situation in which the system administrator trusts the internal users.
- The gateway can be configured to support application -level or proxy service on inbound connections and circuit-level functions for outbound connections.



(c) Circuit-level gateway

# Circuit-Level Firewall

- **Advantage:**

Comparatively inexpensive and provide anonymity to the private network.

- **Disadvantage:**

Do not filter individual packets.

# ***password security***

Password protection is a security process that protects information accessible via computers that needs to be protected from certain users. Password protection allows only those with an authorized password to gain access to certain information.

## Network Security: Password Creation and Use

One of the most important aspects of network security is the use and creation of passwords. Passwords, should be considered top secret. Your network password is the one thing that keeps an impostor from logging on to the network by using your username and therefore receiving the same access rights that you ordinarily have. Guard your password with your life.

## Here are some tips for creating good passwords

- Don't use obvious passwords, such as your last name, your kid's name, or your dog's name.
- 
- Don't pick passwords based on your hobbies, either. A friend of mine is into boating, and his password is the name of his boat. Anyone who knows him can guess his password after a few tries. Five lashes for naming your password after your boat.

- Store your password in your head — not on paper. Especially bad: Writing down your password on a sticky note and sticking it on your computer's monitor. Ten lashes for that. (If you must write down your password, write it on digestible paper that you can swallow after you've memorized the p

- Most network operating systems enable you to set an expiration time for passwords. For example, you can specify that passwords expire after 30 days. When a user's password expires, the user must change it. Your users may consider this process a hassle, but it helps to limit the risk of someone swiping a password and then trying to break into your computer system later.

- You can also configure user accounts so that when they change passwords, they can't specify a password that they've used recently. For example, you can specify that the new password can't be identical to any of the user's past three passwords.

- A new trend is the use of devices that read fingerprints as a way to keep passwords. These devices store your passwords in a secret encoded file, then supply them to the requestor — after the device has read your fingerprint. Fingerprint readers used to be exotic and expensive, but you can now add a fingerprint reader to a computer for as little as $50.

## The Importance of Strong, Secure Passwords

One of the most common ways that hackers break into computers is by guessing passwords. Simple and commonly used passwords enable intruders to easily gain access and control of a com evice.

# Network password security: Following password policy best practices

- There have been many recent stories of major sites, such Facebook, being successfully targeted by hackers , who have managed to collect thousands -- if not hundreds of thousands -- of users' passwords and other user-related information

- The password-protected sites and services he uses all claim to take security seriously and to keep personal details stored securely. But time and again cases occur where usernames, passwords and other personal details are stolen. And what about those sites that look genuine, but are merely a front for harvesting usernames and passwords based on the knowledge that most people use the same combinations for all their accounts? So our careful, security-conscious employee has unwittingly given up his logon credentials for your network and its resources to a variety of untrusted and trusted -- but not necessarily secure -- third parties.

- Organisations that require staff to carry an ID card should look at upgrading those cards to tokens for use in two-factor authentication. This would provide a centralized means to establish and enforce access policies for both physical and logical resources, greatly reducing the risks and costs associated with stolen passwords, as well as blending in with a system employees are already accustomed to.

# Password Hacking

In general, people tend to set passwords that are easy to remember, such as their date of birth, names of family members, mobile numbers, etc. This is what makes the passwords weak and prone to easy hacking.

## A strong password has the following attributes −

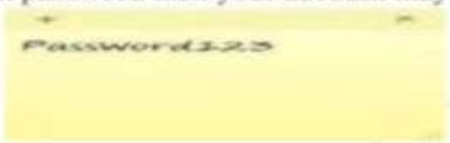
- Contains at least 8 characters.
- 
- A mix of letters, numbers, and special characters.
- 
- A combination of small and capital letters.

## Why We Need Passwords?

- Password is a secret word or code used to serve as a security measure against unauthorized access to data
- Why we need?
- To protect your valuable or personal information on your computer
- To protect your email read by some one else
- To protect your network
- To protect your Website
- To protect your online banking

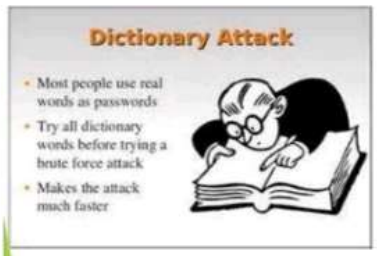
## Weak Passwords

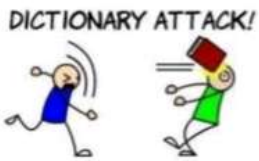
- A password that is easy to detect both by humans and by computer is a weak password
- Short password can be quickly hacked
- Whole dictionary or half dictionary words are easily hacked by dictionary attack
- Reusing old passwords increase the likelihood that your account might be hacked
- Because if someone had one of your old passwords and you've cycled back to using that password then your account may become compromised




## Weak Passwords

## Dictionary Attack




## Brute Force Attack

- Brute force is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys
- Just as a criminal might break into, or "crack" a safe by trying many possible combinations, a brute force cracking application proceeds through all possible combinations of legal characters in sequence
- Like hello, HELLO, Eello, keLLO, FELlo,…


## List of Weak Passwords

1. Your partner, child, or pet's name, possibly followed by a 0 or 1
2. The last 4 digits of your social security number.
3. 123 or 1234 or 123456.
4. password
5. Your city, or college, football team name.
6. Date of birth – yours, your partner's or your child's.
7. money
8. love

## Why create a strong Password?

- Passwords provide the first line of defense against unauthorized access to your computer
- The stronger your password, the more protected your computer will be from hackers and malicious software
- You should make sure you have strong passwords for all accounts on your computer
- If you're using a corporate network, your network administrator might require you to use a strong password

## Choosing A strong Password

**HOW TO CHOOSE A SECURE PASSWORD?**

**HAS AT LEAST 10 CHARACTERS;**
**HAS LOWERCASE LETTERS;**
**HAS SYMBOLS, SUCH AS ` ! " ? $ ? % ^ & * ( ) _ - + = } { [ ] : ; @ ' ~ # | \ < , > . ? /**
**IS NOT YOUR NAME;**
**IS NOT YOUR FRIEND'S NAME;**
**IS NOT A DICTIONARY WORD, SUCH AS APPLE, MYCAR**
**IS NOT A KEYBOARD PATTERN, SUCH AS QWERTY, ASDFGHJKL, OR 12345678.**

## Some Tips

- A password might meet all the criteria above and still be a weak password
- For example, Hello2U!
- It meets all the criteria for a strong password listed above, but is still weak because it contains a complete word
- H3ll0 2 U! is a stronger alternative because it replaces some of the letters in the complete word with numbers and also includes spaces

# DNA CRYPTOGRAPHY

- Recent research considers the use of the Human genome in cryptography

  •The spiritual concepts based on trinity and complementary that is considered in the DNA structure is able to be used in the cryptography process as an alternative technique.
  •The genetic code is based considering codons (consists of 3 nucleic acids from possible 4, as a 64 possible triplets) organised as a dual helix with complementary strands.

- In 2000, the Junior Nobel Prize was awarded to a young Romanian-American student, Viviana Risca, for her work in DNA steganography.

# DNA CRYPTOGRAPHY

- We propose to introduce DNA cryptography into the common PKI scenario
- And encode the medical records of an individual in DNA data strand
- Flanked by unique primer sequences
- Unique primer sequences we obtain in the process of :

  *Deriving DNA Private Key from blood analysis.*

- Using an information conversion program Stefani encodes the medical records of an individual according to CDMB in

***DNA data strand***

flanked by unique primer sequences S1

mixes it among other decoy DNA strands and sends to the receiver through a public channel

- Otto then obtains the unique primer sequences
- That mark the beginning and the end of secret data DNA strand hidden among the decoy strands.
- In this last step, he uses the information conversion program and reads the medical record of the individual.

| METHOD | ADVANTAGE | DISADVANTAGE |
| --- | --- | --- |
| Dna based implementation of encryption. | ○ Real message is not transferred over network.<br>○ scalable for large digital information product. | Size of plaintext increase the encryption And decryption And Time. |
| Dna encryption based on matrix manipulation. | ○ Always get new cipherdata from same plaintext | It include only basic operation and security Only depends on key. |
| | | |