5. Web & System Security

Web Security

Web now widely used by business, goverment, individuals. but internet & web are vulnerable, it have a variety of threat.

- integrity
- confidentiality
- denial of service
- authentication

needed a added security mechanisms.

SSL (Socket Secure Layer)

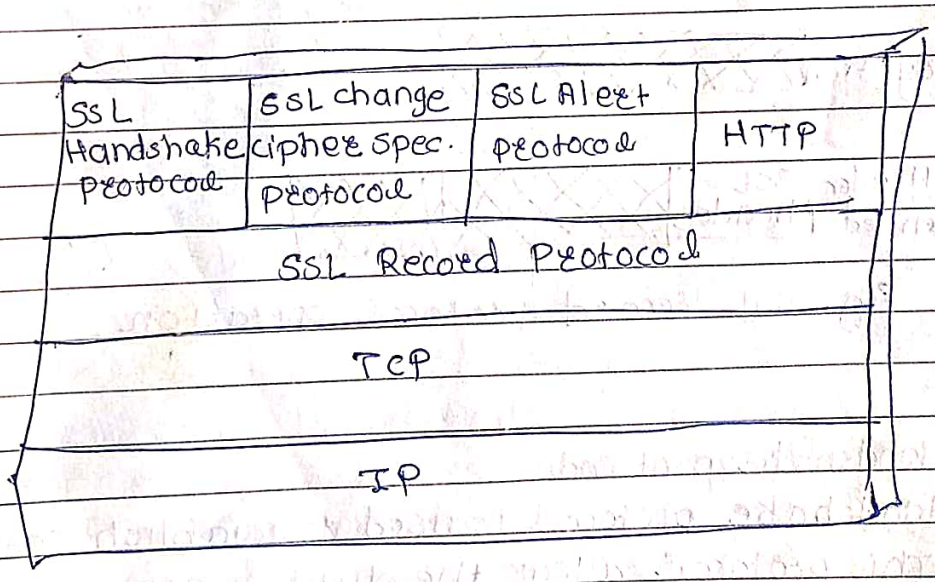
(It is std tech for transmitting doc. securely across n/w, created by Netscape, comm. betn web server & web browsers)

i) It is a transport layer security service it communicate using (TCP protocol)

ii) originally developed by Netscape & version 3 designed with public input subsequently became internet standard known as TLS (Transport layer security) uses TCP to provide a reliable end to end service.

iii) SSL has two layers of protocol.

* SSL Architecture



There are four protocols are present in SSL.

i) SSL record protocol
ii) Handshake protocol
iii) change cipher spec protocol
iv) Alert protocol.

1) SSL Record protocol

i) SSL record provides two services to ssl connection
   a) confidentiality
   b) message integeity.

ii) In that appln data is divided into fragments. the fragment is compressed & then encrypted MAC (Message Authentication Code) generated by algorithm like SHA (secure hash protocol) & MD5 (message digest) is appended.

iii) After that encryption of the data is done & in last SSL header is appended to the data.

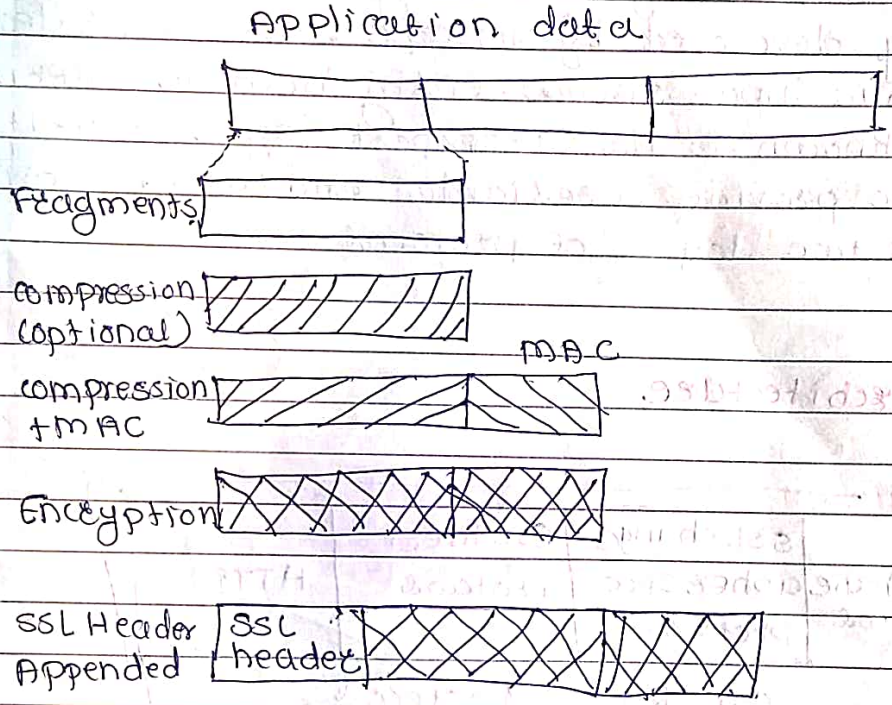


Fig. SSL record protocol operation.

2) Handshake protocol.

i) Handshake protocol is used to establish sessions.

ii) This protocol allows the client & server to authenticate each other by sending a series of msg. to each other.

iii) Handshake protocol uses four phases to complete it's cycle.

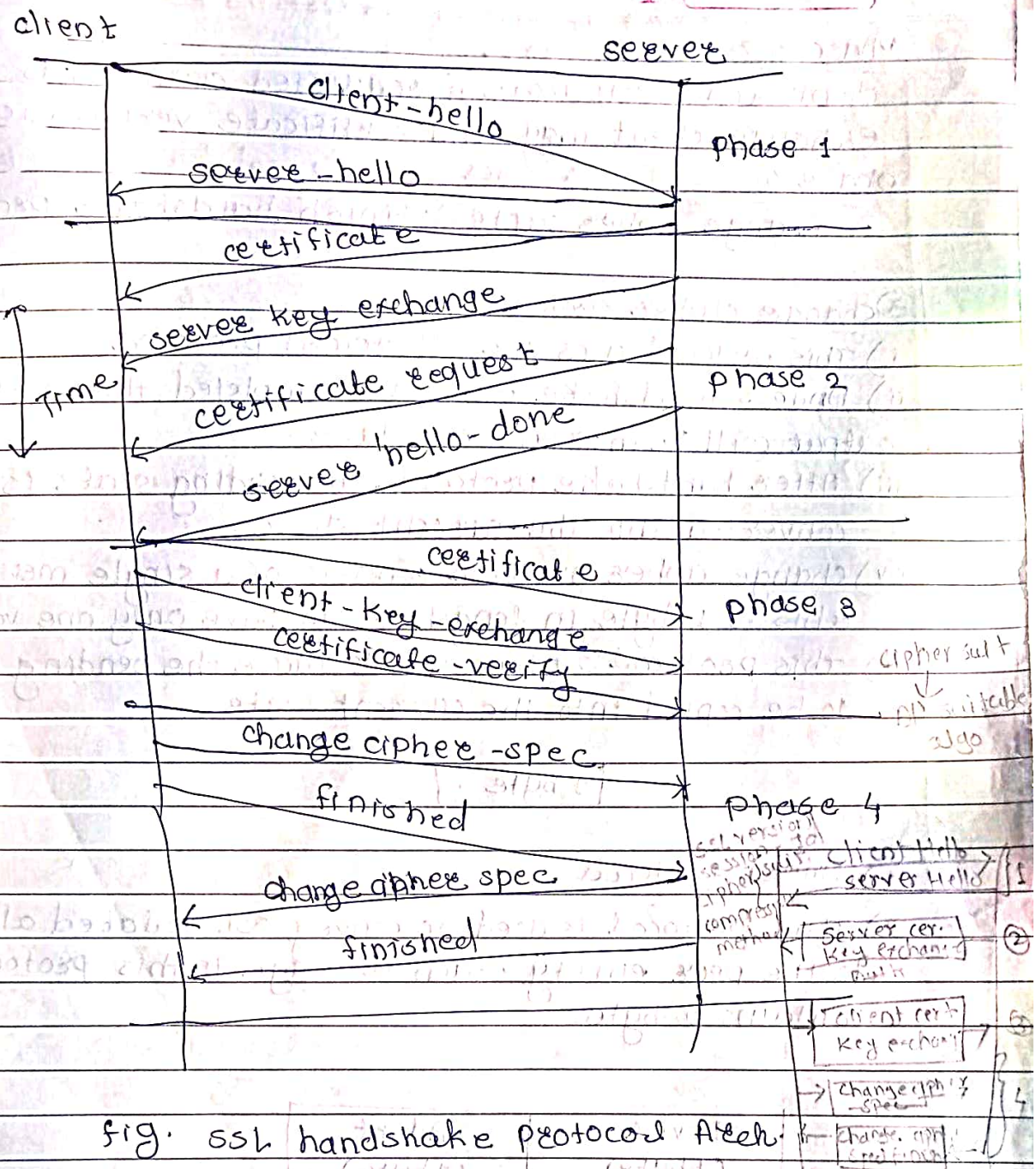


fig. SSL handshake protocol Arch.

Deciding which version of the protocol to use.

* Phase 1 → the system decides which protocol to use. client & server exchange hello packet with each other to confirm Establish Security capabilities including protocol version, session ID, cipher suite, compression method & initial random numbers.

Phase 2

Server may send certificate, key exchange, client may send certificate verification & request certificate, server signal & hello message phase

→ server sends his certificate & server. server end phase 2 by exchanging the

verification - client replies to the server by sending his certificate &

Phase 3 → client exchange key

client sends certificate if requested client sends key exchange, client may send certificate verification.

phase 4 → change cipher suite is passed & all verifications & security checks are done after this handshake

change cipher suite & finish handshake protocol.

3) change cipher protocol

i) This protocol uses the SSL record protocol

ii) Unless handshake protocol is completed, the ssl record output will be in a pending state.

iii) After handshake protocol, the pending state is converted into the current state.

iv) change cipher protocol consists of a single message which is 1 byte in length & can have only one value.

v) This protocol's purpose is to cause the pending state to be copied into the current state.

1 byte.

4) Alert protocol

i) This protocol is used to convey SSL related alerts to the peer entity. Each message in this protocol contains 2 bytes.

Level (1 byte)	Alert (1 byte)

The level is further classified into two parts

1) warning → This alert has no impact on the connection between sender & receiver.

2) Fatal error →

This alert breaks the connection between sender & receiver.

* specific alert

1) unexpected msg., bad record mac, decompression failure, handshake failure, illegal parameter.

2) close notify, no certificate, bad certificate, unsupported certificate, certificate revoked, certificate expired, certificate unknown.

* TLS (Transport Layer security)

i) TLS are designed to provide security at the transport layer. TLS was derived from a security protocol called secure service layer (SSL)

ii) TLS ensures that no third party may evasdropo or tampers with any message.

working of TLS Handshake Mechanism

i) The client connect to server, the client will besomething The client sends no. of specification
   a) version of SSL / TLS
   b) which cipher suites, compression method it wants to use.

ii) The server checks what the highest SSL / TLS version is that is supported by them both, picks a cipher suite from one of the clients option & optionally picks a compression method.

iii) After this the basic setup is done, the server provide it's certificate, this certificate must be trusted either by the client itself or a party that the client trusts.

iv) Having verified the certificate & being certain this server really is who he claims to be key is exchanged; this can be public key or simply nothing depending upon cipher suite.

v) Both the server & client can now compute the key for symmetric encryption. The handshake is finished & the two hosts can communicate securely.

vi) To close a connection by finishing, TCP connection both sides will know the connection was improperly terminated.

vii) The connection can not be compromised by this through merely interrupted.

i) client & s exchange key (DH)
ii) open encrypted channel (DES)
iii) If a session key is not changed

SET (Secure Electronics Transaction)

i) SET is a system that ensures the security & integrity of electronic transactions done using credit cards in a scenario.

ii) SET is not some system that enables payment but it is a security protocol applied to those payments.

iii) It uses different encryption & hashing techniques to secure payments over the internet done through credit card.

Set components

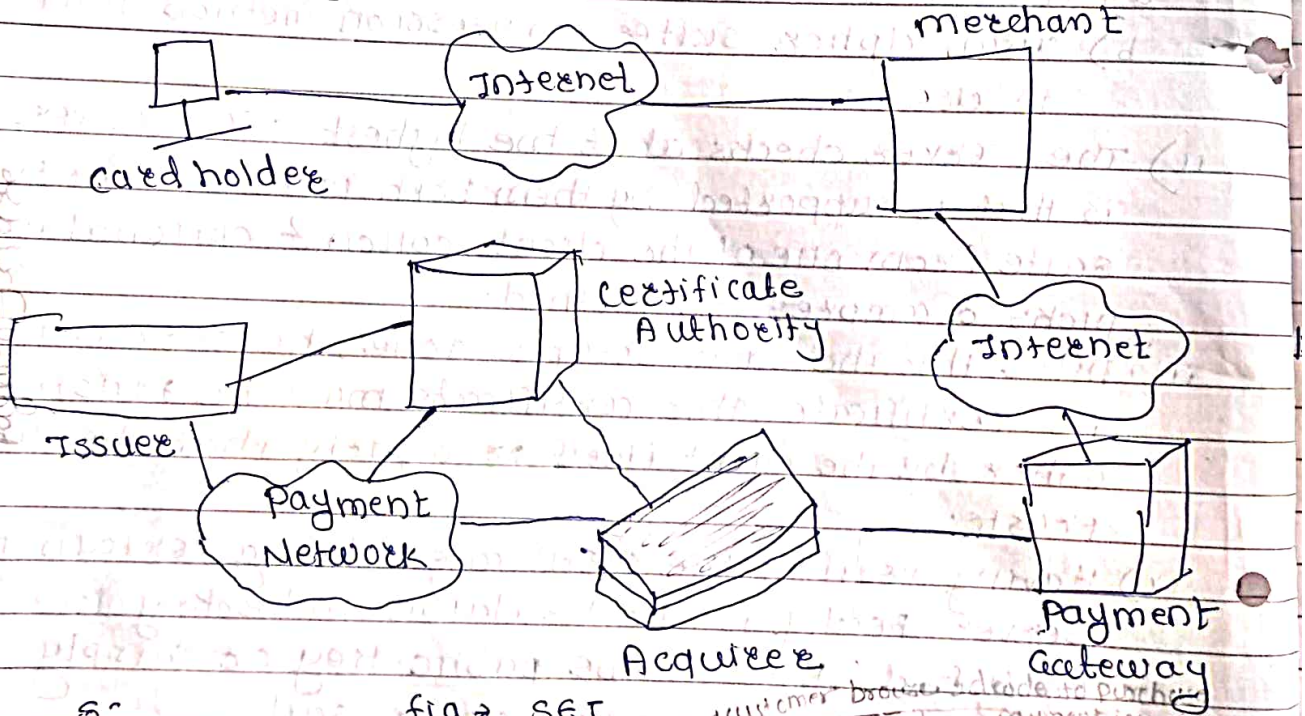


fig → SET

SET Transaction

1) Customer opens account
2) Customer receives a certificate
3) Merchants have their own certificate
4) Customer places an order
5) Merchant is verified
6) Order & payment are sent
7) Merchant requests payment authorization
8) Merchant confirms order
9) merchant provides goods or service.
10) Merchant requests payments.

1. **The customer opens an account.** The customer obtains a credit card account, such as MasterCard or Visa, with a bank that supports electronic payment and SET.
2. **The customer receives a certificate.** After suitable verification of identity, the customer receives an X.509v3 digital certificate, which is signed by the bank. The certificate verifies the customer's RSA public key and its expiration date. It also establishes a relationship, guaranteed by the bank, between the customer's key pair and his or her credit card.
3. **Merchants have their own certificates.** A merchant who accepts a certain brand of card must be in possession of two certificates for two public keys owned by the merchant: one for signing messages, and one for key exchange. The merchant also needs a copy of the payment gateway's public-key certificate.
4. **The customer places an order.** This is a process that may involve the customer first browsing through the merchant's Web site to select items and determine the price. The customer then sends a list of the items to be purchased to the merchant, who returns an order form containing the list of items, their price, a total price, and an order number.
5. **The merchant is verified.** In addition to the order form, the merchant sends a copy of its certificate, so that the customer can verify that he or she is dealing with a valid store.
6. **The order and payment are sent.** The customer sends both order and payment information to the merchant, along with the customer's certificate. The order confirms the purchase of the items in the order form. The payment contains credit card details. The payment information is encrypted in such a way that it cannot be read by the merchant. The customer's certificate enables the merchant to verify the customer.
7. **The merchant requests payment authorization.** The merchant sends the payment information to the payment gateway, requesting authorization that the customer's available credit is sufficient for this purchase.
8. **The merchant confirms the order.** The merchant sends confirmation of the order to the customer.
9. **The merchant provides the goods or service.** The merchant ships the goods or provides the service to the customer.
10. **The merchant requests payment.** This request is sent to the payment gateway, which handles all of the payment processing.

SET Requirements:

1. **Provide confidentiality of payment and ordering information:** It is necessary to assure cardholders that this information is safe and accessible only to the intended recipient.

Confidentiality also reduces the risk of fraud by either party to the transaction or by malicious third parties. SET uses encryption to provide confidentiality.

2. **Ensure the integrity of all transmitted data:** That is, ensure that no changes in content occur during transmission of SET messages. Digital signatures are used to provide integrity.
3. **Provide authentication that a cardholder is a legitimate user of a credit card account:** A mechanism that links a cardholder to a specific account number reduces the incidence of fraud and the overall cost of payment processing. Digital signatures and certificates are used to verify that a cardholder is a legitimate user of a valid account.
4. **Provide authentication that a merchant can accept credit card transactions through its relationship with a financial institution:** This is the complement to the preceding requirement. Cardholders need to be able to identify merchants with whom they can conduct secure transactions. Again, digital signatures and certificates are used.
5. **Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction:** SET is a well-tested specification based on highly secure cryptographic algorithms and protocols.
6. **Create a protocol that neither depends on transport security mechanisms nor prevents their use:** SET can securely operate over a "raw" TCP/IP stack. However, SET does not interfere with the use of other security mechanisms, such as IPSec and SSL/TLS.
7. **Facilitate and encourage interoperability among software and network providers:** The SET protocols and formats are independent of hardware platform, operating system, and Web software.

PAGE :
DATE : / /

* Participants in SET

In general scenario of online transactions, SET includes similar participants.

1) cardholder - customer
2) Issuer - customer financial institution
3) Merchant
4) Acquer - Merchant financial
5) certificate authority - Authority that follows certain standards & issues certificates to all other participants.

SET functionality

1) Provide authentication

a) Merchant authentication

To prevent theft, SET allows customers to check previous relationships between merchants & financial institutions.

b) Customer / cardholder authentication

SET checks if the use of credit card is done by an authorized user or not using x.509 v3 certificate.

2) Provide message confidentiality

confidentiality refers to preventing unintended people from reading the message being transferred. SET implements confidentiality by using encryption techniques.

3) Provide message integrity

SET doesn't allow msg. modification with the help of signatures. Msg. are protected against unauthorized modification using RSA digital signature with SHA-1 & some using HMAC with SHA-1.

4) Dual signature

Dual signature is a concept introduced with SET, which aims at connecting two info. pieces meant for two different receivers.

a) Order info. (OI) for merchant
b) Payment info. (PI) for bank

* Intruders

One of the most publicized attack to security is the intruder generally referred to as hacker or cracker.
Three classes of intruders are as follows.
1)

1) Masquerader

An individual who is not authorized to use the computer & who penetrates a system's access controls to exploit a legitimate users account.
↓ कायदेशीर

2) Misfeasor

A legitimate user who accesses data, programs or resource for which such access is not authorized or who is authorized for such access but misuse his or her privileges.

3) Clandestine user

An individual who seizes supervisory control of the system & uses this control to evade auditing & access controls or to supress audit collection.

- Intruder attack range from the benign to the serious. At the benign end of the scale, there are many people who simply wish to explore internets & see what is out there.
- At the serious end are individuals who are attempting to read privileged data, perform unauthorized modifications to data or disrupt the system.
- Benign intruders might be tolerable, although they do consume resources & may slow performance for legitimate users, however there is no way in advance to know whether an intruder will be benign or malign.

* Intruder techniques

The objective of the intruders is to gain access to a system or to increase the range of privileges accessible on a system. Generally this requires the intruders to acquire info. that should be protected. In most case the info. is in the form of user password.

Typically a system must maintain a file that associates a password with each authorized user. If such file is stored with no protection, then it is easy matter to gain access to it. The pasword files can be protected in on of the two ways.

1) One way encryption

The system stores only an encrypted form of user's password. In practice, the system usually performs a one way transformation in which the password is used to generate key for the encryption function & in which fixed length output is produced.

2) Access control

Access to the password file is limited to one or very few accounts.

Intruder Detection

Inevitably the best intrusion prevention system will fail. a systems second line of defense is intrusion detection & this has been focus of much research in recent years. This interest is motivated by no. of considerations including the following.

a) If an intrusion is detected quickly enough, the intruder can be identified & ejected from the system before any damage is done or any data are compromised.

b) An effective intrusion detection system can serve as a deterrent so acting to prevent intrusions.

c) Intrusion detection enables the collection of info. about intrusion tech. that can be used to strengthen the intrusion prevention facility.

Figure suggest a very abstract terms, the nature of task confronting the designer of an intrusion detection system. Although typical behavior of an intruder differs from the typical behavior of an authorized user, there is an overlap in these behaviors. Thus a loose interpretation of intruder behavior which will catch more intruders will also lead to a no. of 'false +ve'

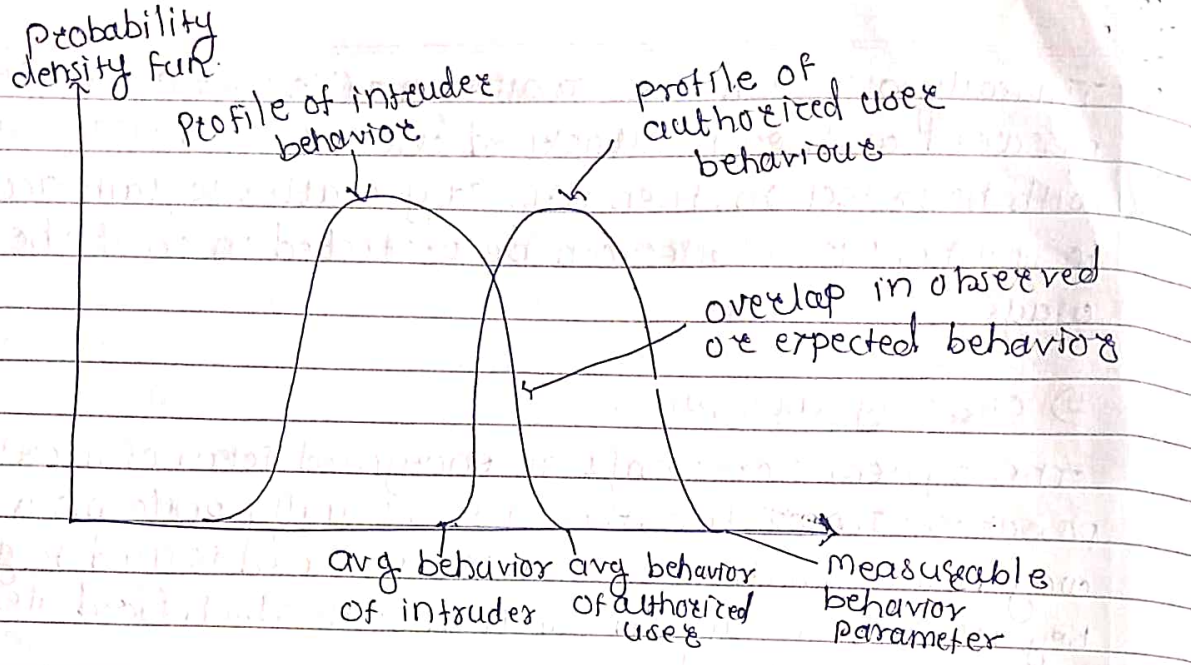


fig. Profiles of behavior of intruders & authorized users.

** Approaches to intrusion Detection

1) stastical anomaly detection

i) It involves the collection of data relating to the behavior of legitimate users over period of time. Then stastical test are applied to observed behavior to determine with high level of confidence whether that behavior is not legitmate user behavior

a) Threshold detection

It involves defining threshold, independent of user for the frequency of occurrence of various events.

b) Profile based

A profile of the activity of each user is developed & used to detect changes in the behaviour of individual accounts

2) Rule based detection

It involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.

a) anomaly detection → Rules are developed to detect deviation from previous usage pattern.

b) Penetration identification → An expert system approach that searches for suspicious behavior.

3) Statical Anomaly detection

i) Statical detection techniques fall into two broad categories, threshold detection & profile based system.

ii) Threshold detection involves counting the no. of occurrences of specific event type over an interval of time.

iv) If the count surpasses what is considered a reasonable no. that one might expect to occur then intrusion is assumed.

4) Profile based anomaly

Examples of metrics that are useful for profile based intrusion detection are the following.

i) Counter → A nonegative integer that may be incremented but not decremented until it is reset by mgmt action.

2) Gauge →

A nonnegative integer that may be incremented or decremented.

3) Interval time → The length of time between two related events.

9.) The hashed password is then stored, together with a plaintext copy of the salt, in password file for the corresponding user ID.

10.) This method has been shown to be secure against a variety of cryptanalytic attack.

* Password selection strategies

Four basic techniques are in use.

i) User education
ii) Computer generated passwords
iii) Reactive password checking
iv) Proactive password checking.

① User education strategy is unlikely to succeed at most installation, particularly where there is a large user population or a lot of turnover → many will simply ignore the guidelines.

② Computer generated passwords also have problems. If the passwords are quite random in nature, users will not be able to remember them. Even if the password is pronounceable, the user may have difficulty remembering it and so be tempted to write it down

③ A reactive password checking strategy is one in which the system periodically runs its own password cracker to find guessable passwords.

④ In proactive password checker user is allowed to select his or her own password.

* Trusted system

- one way to enhance the ability of a system to defend against intruders & malicious programs is to implement trusted system technology.

Data access control

- Following successful logon, the user has been granted access to on set of hosts & appln.
- This is generally not sufficient for system that includes sensitive data in its database.
- Through the user access control procedure, user can be identified to the system. Associated with each user there can be profile that specifies permissible operⁿ & file accesses.
- The os can then can be then enforce rules based on the user profile.

A general model of access control as exercised by an file or DBMS is that of an access matrix. The basic elements of the model as follows.

1) Subjects

An entity capable of accessing objects. Generally the concept of subject equates with that of process.

2) Object

Anything to which access is controlled. Examples include files, portion of files, programs & segments of memory.

3) Access right

The way in which the object is accessed by subject examples are read, write, execute.

	Program 1	...	Segment A	Segment B
Process 1	Read		Read	
process 2	Execute		write	
				Read

Access control list for program 1 : Process 1 (Read, Execute)
Access control list for segment A : process 1 (Read, write)
Access control list for segment B : Process 2 (Read)

a) Access matrix

Capability list for Process 1 : Program 1 (Read, Execute) Segment A (Read)
capability list for process 2 : segment B (Read)

b) Access control list.

fig. Access control structure

* when multiple categories or levels of data are defined the requirement is referred to as multilevel security. The general statement of the requirement for multilevel security is that a subject at high level may not convey info. to a subject at lower or noncomparable level unless that flow accurately is in two parts & is simply stated A multilevel secure system must enforce

1) No read up.

A subject can only read an object of less or equal security level. This is referred to as simple security property.

2) No write down

A subject can only write into an object of greater or equal security level.

* Firewall

i) Internet connectivity is no longer an option for most organizations.

ii) However while internet access provides benefits to the org. it enables the outside world to reach & interac with local networks assets.

iii) This creates threat to the org. while it is possible to to equip each workstation & server on the premises nlw with strong security features, such as intrusion protectio this is not practical approach

iv) The firewall is inserted between the premise networ & internet to establish a controlled link & to erect an outer security wall or perimeter. The aim of this perimeter is to protect the premises network from internet based attack & to provide single choke point where security & audit can be imposed.

v) The firewall can be a single computer system or a set of two or more systems that cooperate to perform the firewall function.

* Firewall characteristics

1) All traffic from inside to outside & vice versa must pass through the firewall.

2) only authorized traffic, as defined by the local security policy, will be allowed to pass various types of firewalls are used.

3) The firewall itself is immune to penetration. This implies that use of trusted system with secure os.

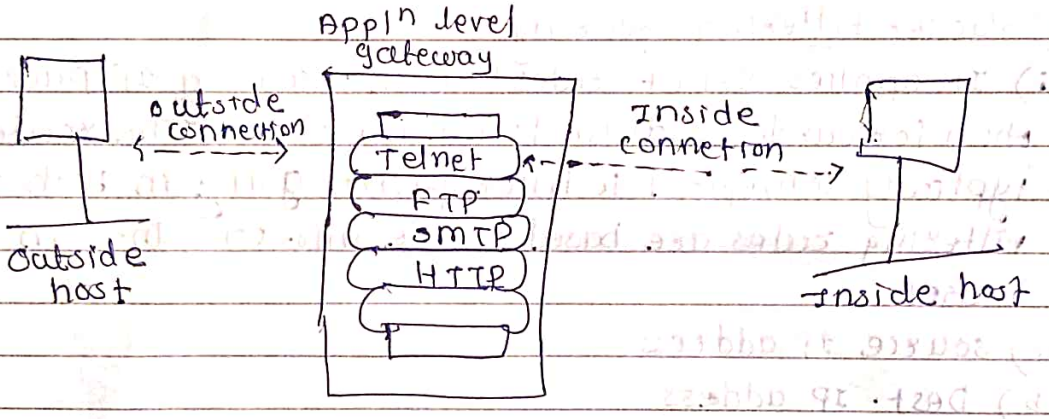
* Four techniques that firewall use to control access

1) service control

Determines the type of internet services that can be accessed, inbound or outbound. The firewall may filter traffic on this basis of IP address & TCP port no may provide proxy slw that receives & interprets each service request before passing it on or may host the server slw itself such as web or mail service.

2) Application level gateway

i) An appln level gateway also called a proxy server, acts as relay of appln level traffic
ii) The user contacts the gateway using TCP/IP appln such as Telnet or FTP & the gateway asks the user for the name of the remote host to be accessed.
iii) when the user respond & provides valid user id & authentication info., the gateway contacts the appln on the remote host & relays TCP segments containing appln data beth two endpoints
iv) It tend to be more secure than packet filters.
v) It is easy to log & audit all incoming traffic at the appln level.
vi) A prime disadvantage is the additional processing overhead on each connection.

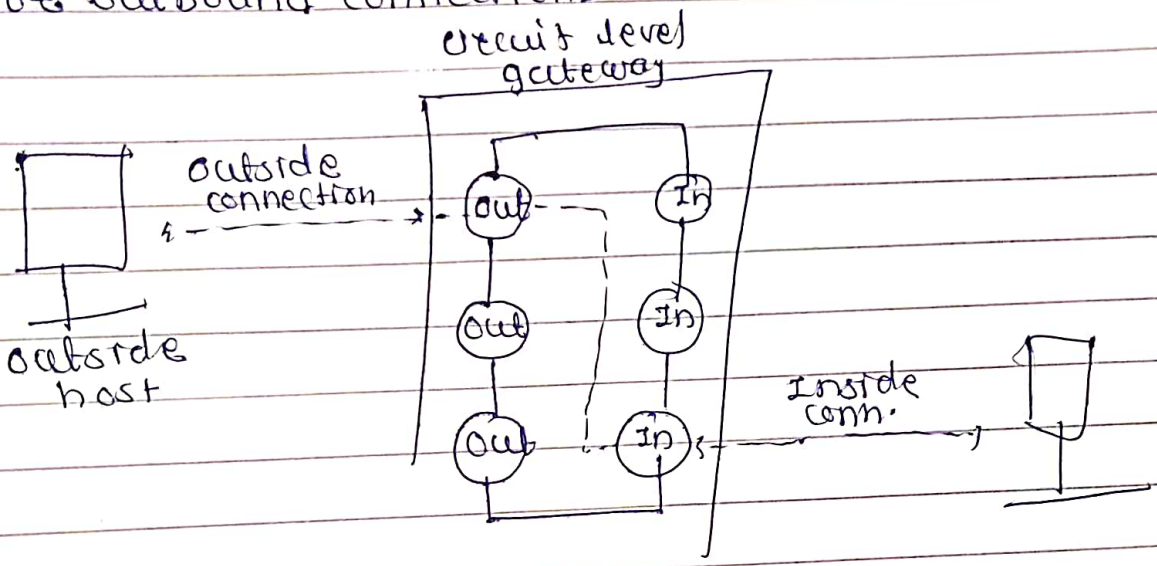


b) Appln. level gateway

3) Circuit level gateway

i) It can be stand alone system or it can be specified functio performed by an appln. level gateway for certain appln.
ii) A circuit level gateway does not permit end to end TCP connection rather the gateway set up two TCP connectio on beth itself & TCP used on an inner host & one beth itself & TCP user on an outer host
iii) once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents.

A typical use of circuit level gateways is a situation in which the system administrator trust the internal users. The gateway can be configured to support appln level or proxy service on inbound connections & circuit level functions for outbound connections



a) circuit level gateway.