Information Security

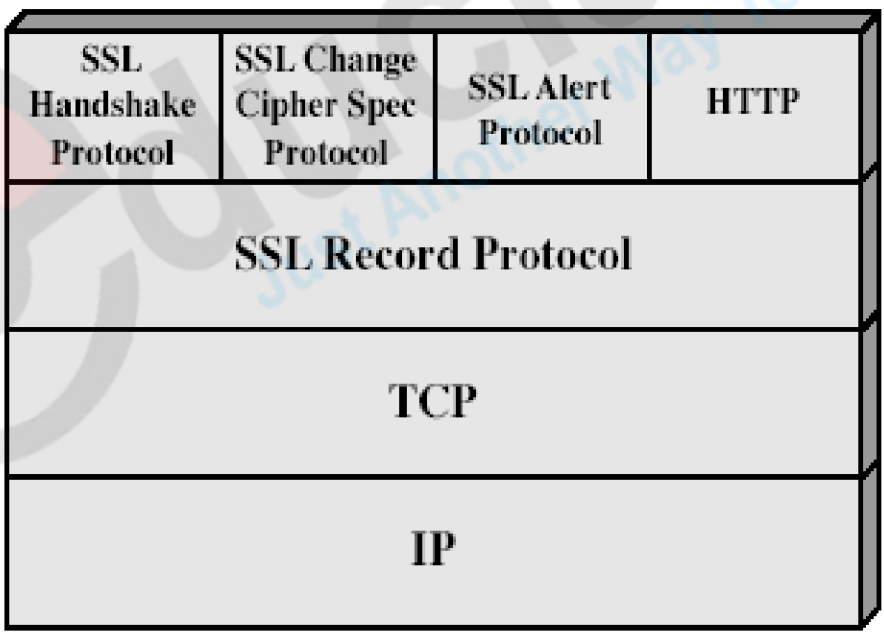
1. Explain SSL process

- It is an internet protocol for secure exchange of information between web browser and web server
- Two basic services

  - authentication

  - confidentiality
- Three versions: 2, 3, 3.1

  Most popular - version 3
- uses TCP to provide a reliable end-to-end service



- SSL record protocol provides basic security services to various higher layer protocols
- HTTP provides transfer service for Web client/server interaction

- The handshake protocol, Change Cipher Spec protocol and Alert protocol are used in the management of SSL exchanges

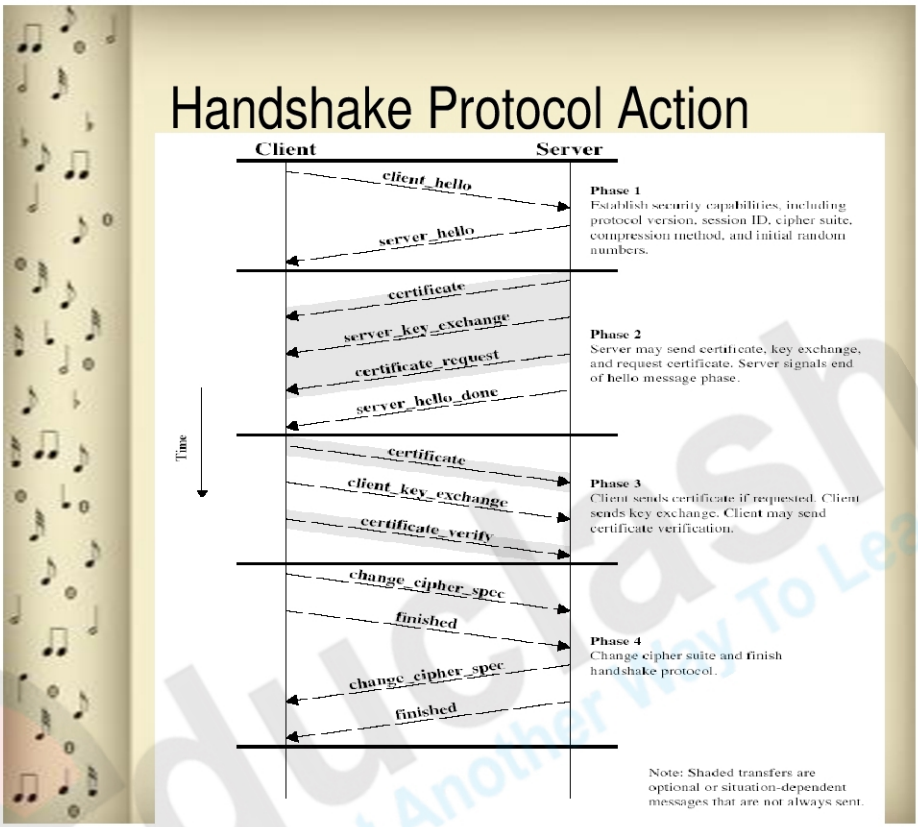
Two important concepts of SSL

1. SSL Connection
2. SSL Session

- **SSL session**
  - an association between client & server
  - created by the Handshake Protocol
  - may be shared by multiple SSL connections
  - **SSL connection**
  - a transient, peer-to-peer, communications link
  - associated with 1 SSL session

Handshake Protocol

- This protocol allows the server and client to authenticate each other
- This protocol is used before any application data are transmitted
- It consist of a series of messages exchanged by client and server
- Each message has three fields
  1. Type - 1 byte
  2. Length - 3 bytes
  3. Content - ≥ 1 byte
- Exchange establish a logical connection between client and server
- Four phases are involved
  - Establish Security Capabilities
  - Server Authentication and Key Exchange
  - Client Authentication and Key Exchange
  - Finish



Phase 1. Establish security capabilities

- It is used to initiate a logical connection and to establish the security capabilities
- Client initiates the exchange
- Client sends a client_hello message
- The parameters included in the message are

    1.Version

    2.Random

    3.Session ID

    4.CipherSuite

    5.Compression Method

- After sending the client_hello message, the client waits for the server_hello message
- Server_hello message contains the same parameters of the client_hello message

Phase2 : Server Authentication and Key Exchange

- Server begins the phase by sending its certificate
- Message contains one or a chain of X.509 certificates
- This message is needed for agreed key exchange method
- Aserver_key_exchangemessage
  is send to the client
- Then a certificate_request message is send to the client
- This message includes two parameters
    1. certifcate_type
    2. certificate_authorities
- The certificate type indicates the public key algorithm and its use
- The certificate authorities is a list of distinguished names of acceptable certificate authorities
- Then a server_done message is send
- It indicates the end of the server hello and associated messages
- After sending this message, the server will wait for clients response

Phase3 : Client Authentication and Key Exchange

- After getting the server_done message, the client verify whether the server has provided a valid certificate
- Then check whether the server_hello parameters are acceptable
- The client begins the phase by sending a certificate message
- Then the client_key_exchange message is send
- Finally client send a certificate_verify message to provide explicit verification of a client certificate

Phase4: Finish

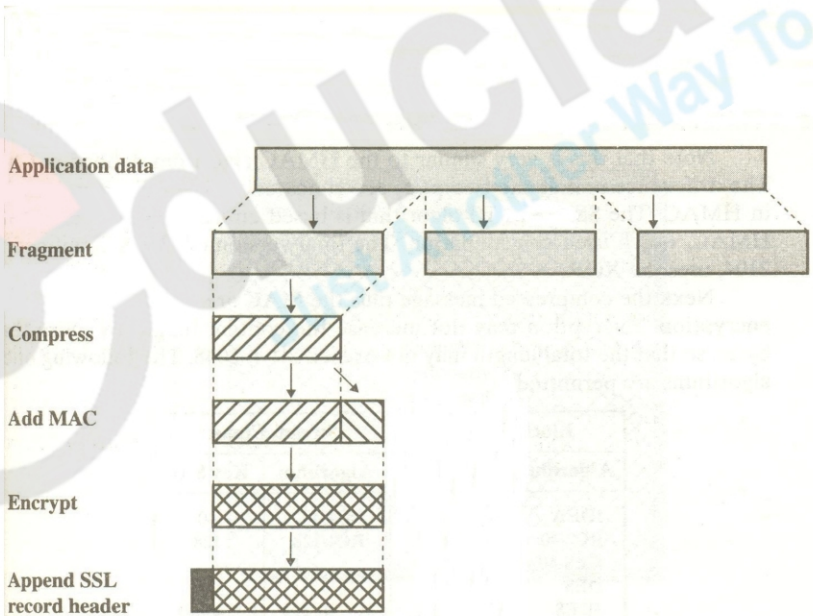
- This phase completes the setting up of a secure connection

- The client sends a change_cipher_spec message to the server
- Then the client will send the finished message
- In response to these two messages, the server sends its own change_cipher_spec message
- And then sends the finished message
- At this point the handshake is complete
- Then the client and server may begin to exchange data

SSL Record Protocol

- SSL Record Protocol provides two services for SSL connection
- 1. Confidentiality
- 2. Message Integrity

SSL Record Protocol Operation



SSL Record Protocol Operation

Change Cipher Spec Protocol

- It is the simplest protocol that uses the SSL Record Protocol
- It consists of a single message, which consists of a single byte with the value 1
- The purpose of this message is to cause the pending state to be copied into current state

Alert Protocol

- If any error is occurring, the detecting party will create an alert message
- Each message in this protocol consists of two bytes
- First byte takes the value
  - warning(1) or
  - fatal(2)
- If the level is fatal, SSL terminates the connection
- The second byte contains a code that indicates the specific alert

2. Explain in detail E-mail security

- Electronic mail is the most commonly used network based application
- With the increased use of email, the need for providing security is also increased
- Three main protocols
  - PGP
  - S/MIME
  - PEM

Pretty Good Privacy (PGP)

- It is a freely available software package for email security
- Provides confidentiality and authentication service for email
- selected best available crypto algorithm to use
- Integrate it into a program or application
- originally free, now have commercial versions available also

PGP operations

1. Digital signature
2. Encryption
3. Compression
4. Enveloping
5. Base-64 encoding

Operation of PGP consists of five services

1. Authentication
2. Confidentiality
3. Compression
4. E-mail compatibility
5. Segmentation

PGP Operation – Authentication

1. Sender creates a message
2. SHA-1 used to generate 160-bit hash code of message
3. hash code is encrypted with RSA using senders private key, and result is attached to message
4. receiver uses RSA to decrypt using senders public key and recover hash code
5. receiver generates new hash code for message and compares with decrypted hash code, if match, message is accepted as authentic

PGP Operation – Confidentiality

1. sender generates message and random 128-bit number to be used as session key
2. message is encrypted, using CAST-128 / IDEA
3. session key is encrypted using RSA with recipient's public key, then attached to message
4. receiver uses RSA with its private key to decrypt and recover session key
5. session key is used to decrypt message

PGP Operation – Confidentiality & Authentication

- uses both services on same message

- create signature (his private key) & attach to message
- encrypt both message & signature(session key)
- attach RSA encrypted session key(receivers public key)

PGP Operation – Compression

- compresses message after signing but before encrypting
  - so can store uncompressed message & signature for later verification
  - & because compression is non deterministic
  - Encryption is done after compression for providing security
- uses ZIP compression algorithm

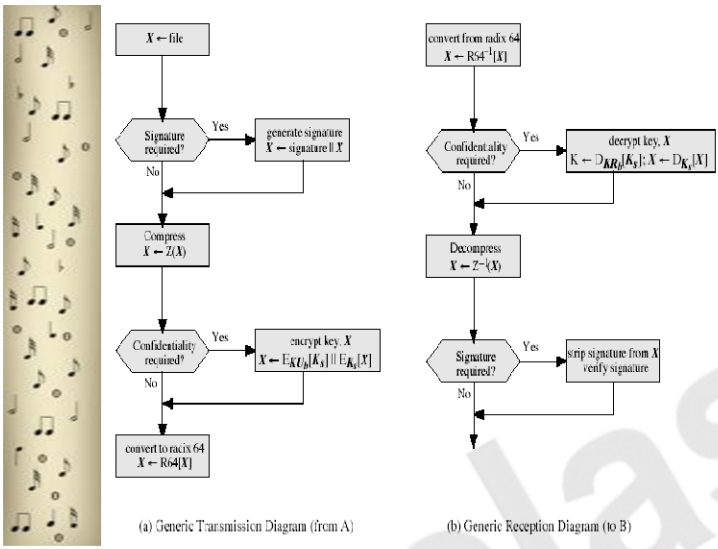
PGP Operation – Email Compatibility

- when using PGP binary data have to be send (encrypted message)
- many email systems are designed only for text
- hence PGP must encode binary data into printable ASCII characters
- uses radix-64 algorithm
  - maps 3 octets of binary data to 4 printable chars
  - also appends a CRC to detect errors

PGP Operation – segmentation

- Email facilities are restricted to maximum message length
- To restrict this, PGP sub divides a message into segments if it is to big
- At the receiving end it will performing reassembling also

PGP Operation – Summary



(a) Generic Transmission Diagram (from A)

(b) Generic Reception Diagram (to B)

PGP Session Keys

- need a session key for each message
  - of varying sizes: 56-bit DES, 128-bit CAST or IDEA, 168-bit Triple-DES
  - uses random inputs taken from previous session key and from keystroke timing of user

PGP Public & Private Keys

- since many public/private keys may be in use, need to identify which is actually used to encrypt session key in a message
  - could send full public-key with every message
  - but this is inefficient
  - rather use a key identifier based on key
  - is least significant 64-bits of the key
  - will very likely be unique at least with in one user
  - also use key ID in signatures

PGP Key Rings

- each PGP user has a pair of key rings:
  - public-key ring contains all the public-keys of other PGP users known to this user, indexed by key ID
  - private-key ring contains the public/private key pair(s) for this user, indexed by key ID

PGP Key Management

- rather than relying on certificate authorities
- in PGP every user is own CA
  - can sign keys for users they know directly
- forms a "web of trust"
  - trust keys have signed
  - can trust keys others have signed if have a chain of signatures to them users can also revoke their keys

S/MIME (Secure/Multipurpose Internet Mail Extensions)

- security enhancement to MIME email format standard
  - original email format standard RFC 822 was text only
  - MIME provided support for varying content types and multi-part messages
  - S/MIME added security enhancements
  - have S/MIME support in various modern mail agents: MS Outlook, Netscape etc
- S/MIME emerge as industry standard for commercial and organizational use
- PGP is used as personal email security for many users

S/MIME Functions

- enveloped data
  - encrypted content and key encrypted with receivers public key
- signed data
  - Message digest encrypted with senders private key
  - Content plus signature is encoded using base64 encoding
- clear-signed data

- Digital signature is performed
- Only digital signature is encoded using base64

- signed & enveloped data
  - nesting of signed & encrypted entities

S/MIME Cryptographic Algorithms

- Message Digest: must support MD5 and SHA-1

  : should use SHA-1

- Digital signature: must support DSS

  : should support RSA

- Enveloping : must support Diffie- Hellmann

  : should support RSA

- Symmetric key encryption : sender

  should support DES-3 and RC4

  : receiver must support

  DES-3 and should support RC2

S/MIME Certificate Processing

- S/MIME uses X.509 v3 certificates
- each client has a list of trusted CA's certs
- and own public/private key pairs & certs
- certificates must be signed by trusted CA's

Key management functions

1. key generation
2. Registration
3. Certificate storage and retrieval

Certificate Authorities

- have several well-known CA's
- VeriSign one of most widely used
- with increasing levels of checks & hence trust

Class	Identity Checks	Usage
1	name/email check	web browsing/email
2	enroll/addr check	email, s/w validate
3	ID documents	e-banking/service access

3. Discuss the security provided at the IP layer in the TCP/IP protocol

- IP packets contain data in plain text form
- Anyone watching IP packets pass by can access them, read their contents and even change them
- The protocol used for providing security at the IP level is called as IP Security(IPSec)
- Idea of IPSec is to encrypt and seal transport and application layer data during transmission
- It also offers integrity protection for the internet layer
- IPSec is a capability that can be added to IPV4 or IPV6, by means of additional headers
- It encompasses three functional areas
    1. Authentication
    2. Confidentiality
    3. Key management

Benefits of IPSec

- IPSec is transparent to end users
- IPSec implemented in a firewall provides strong security
- IPSec allows interconnectivity between branches/offices in a inexpensive manner

IPSec Protocols

- IPSec features are implemented in the form of additional IP Header, known as Extension Header
- Extension headers follow standard IP header
- Offers two main services
    - authentication
    - confidentiality
- Two extension headers are used to support two services

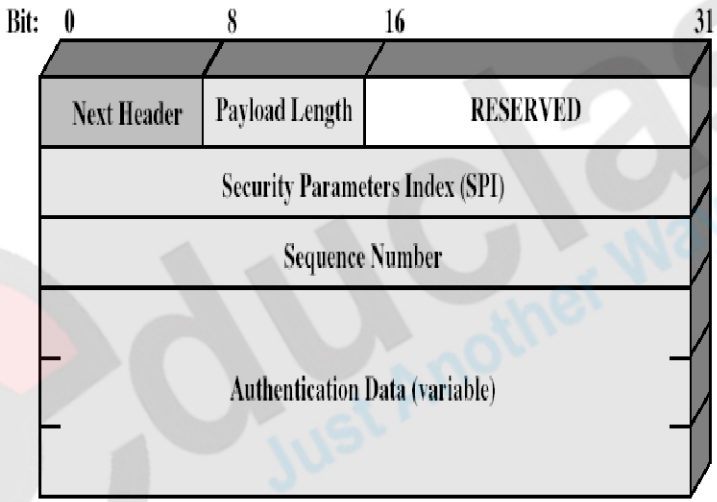
- IPSec consists of two main protocols

    1. Authentication Header (AH)

    2. Encapsulating Security Payload(ESP)

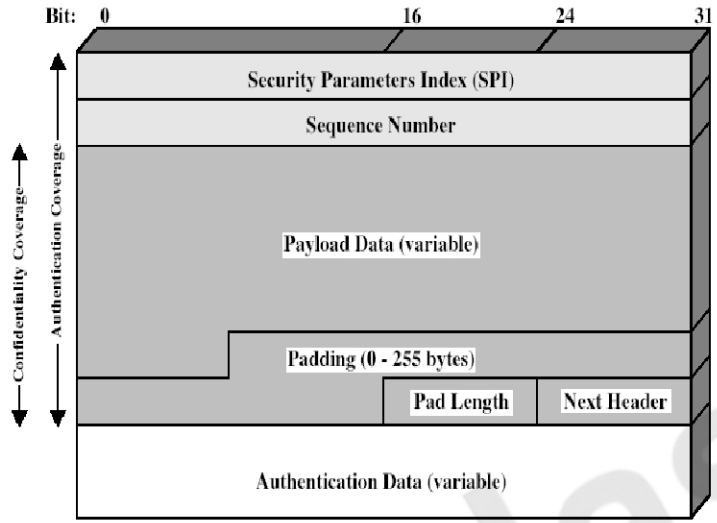
Authentication Header

- provides authentication, integrity and an optional anti-replay service
- AH is a header in an IP packet, which contains a cryptographic checksum for the contents of the packet
- Is inserted between IP header and packet content



Encapsulating Security Payload

- Provides data confidentiality
- New header is inserted into IP Packet
- It transforms data in to encrypted form
- It can be used in isolation or combined with AH



Modes of operation

- Both AH and ESP can be used in two modes

  1. Tunnel mode
  2. Transport mode

Tunnel mode

- it protects the entire IP datagram

- takes an IP datagram, adds IPSec header and trailer and encrypts the whole thing and adds new IP header

-normally used between two routers, a host and a router or a router and a host

Transport mode

- takes transport layer payload, adds IPSec header and trailer and encrypts the whole thing and adds the IP header

- Normally used in host to host (end-to-end)

Internet Key Exchange Protocol

- Protocol used for key management procedures

- IKE is used to negotiate the cryptographic algorithms
- IKE is the initial phase of IPSec
- After IKE , AH and ESP protocols take over
- IPSec is independent of lower level cryptographic algorithms

Security Associations

- It is an agreement between communicating parties about factors such as IPSec protocol version, mode of operation, cryptographic algorithms, keys etc
- SA is unidirectional
- For storing SA, standard storage area called as Security Association Database (SAD) is used by IPSec
- SA is identified by 3 parameters:
- Security Parameters Index (SPI)
- IP Destination Address
- Security Protocol Identifier

Key Management

- handles key generation & distribution
- typically need 2 pairs of keys
  - Two keys for AH & two for ESP
  - One used for message transmission and one for message receiving

Two types of key management

1.manual key management

  - Sys admin manually configures every system

2.automated key management

  - automated system enables on demand creation of keys for SA's in large systems
  - has Oakley & ISAKMP elements

Oakley

- a key exchange protocol
- based on Diffie-Hellman key exchange

- adds features to address weaknesses of diffie hellmann

Features of Oakley

1. defeat replay attack
2. implements a mechanism called as cookies to defeat congestion attack
3. provides authentication to prevent man-in-the- middle attack

ISAKMP

- Internet Security Association and Key Management Protocol
- provides framework for key management
- defines procedures and formats to establish, maintain, modify, & delete SA information

4. Explain the security mechanism used in an electronic transaction

SET: Secure Electronic Transaction

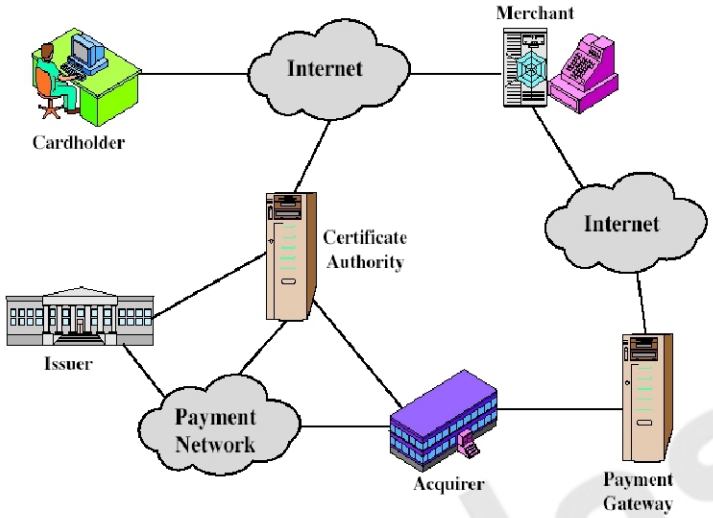
- It is an open encryption and security specification to protect credit card transactions on the internet
- It is a set of security protocols and formats that allows users to use card payment infrastructure in internet securely.

SET provides three services

- Provides a secure communications channel among all parties involved in a transaction
- Provides authentication by the use of digital certificates
- Ensures confidentiality by restricted information to those who need it

SET Participants

1. Cardholder
2. Merchant
3. Issuer
4. Acquirer
5. Payment gateway
6. Certification authority



SET Process

1. customer opens account
2. customer receives a certificate
3. merchants have their own certificates
4. customer places an order
5. merchant is verified
6. order and payment details are sent
7. merchant requests payment authorization
8. Payment gateway authorizes the payment
9. merchant confirms order
10. merchant provides goods or service
11. merchant requests payment

Payment Processing

- It includes

    1. Purchase request

2. Payment authorization

3. Payment capture

Purchase Request

- Before the Purchase Request exchange begins the card holder has completed browsing , selecting and ordering
- Purchase Request exchange consists of four messages
  - Initiate Request
  - Initiate Response
  - Purchase Request
  - Purchase Response

Initiate Request

- Customer request for
  - certificates of the merchant
  - certificate of the payment gateway
- customer will also
  - send his credit card issuer's name
  - unique id and
  - a nonce

Initiate Response

- Merchant creates a message which includes
  - nonce from customer
  - another nonce for customer to return in next message
  - transaction id
- Entire message is encrypted using merchants private key
- Along with message, merchants and payment gateways certificates also

Purchase Request

- Customer

  - verifies the certificates

  - creates OI (Order Information) and

    PI (Payment Information)

- Both OI and PI contains transaction id
- OI contains reference to customers order given before
- PI contains details such as credit card number, expiry and purchase amount
- Then customer prepare purchase request

Purchase request includes

- 1. Purchase-related information
- 2. Order-related information
- 3. Cardholder certificate

Purchase-related information

- This is forwarded to the payment gateway by the merchant
- It consist of

- PI
- dual signature calculated over the PI and OI
- OI message digest (OIMD)
- all these encrypted with random key **K**
- digital envelope(**K** encrypted using

  payment gateways public key)

Order-related information

- This information is needed by the merchant
- Consists of

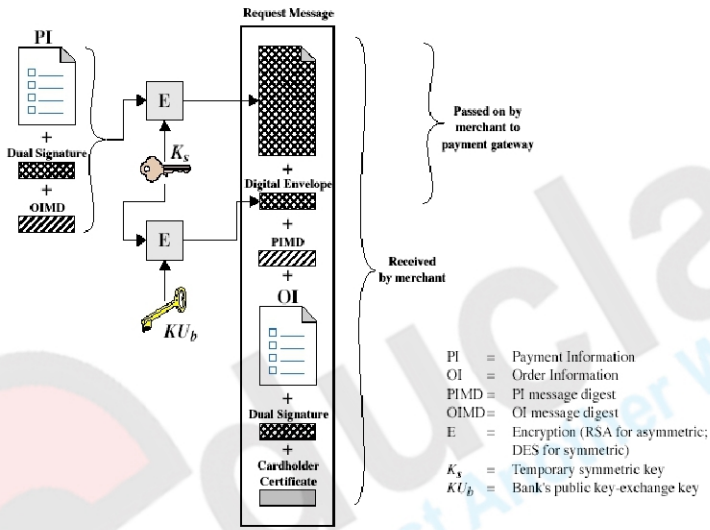
- OI

- dual signature computed over PI and OI
- PIMD

Cardholder certificate

- This contains the cardholder's public key
- Is needed by the merchant and by the payment gateway

Purchase Request – Customer

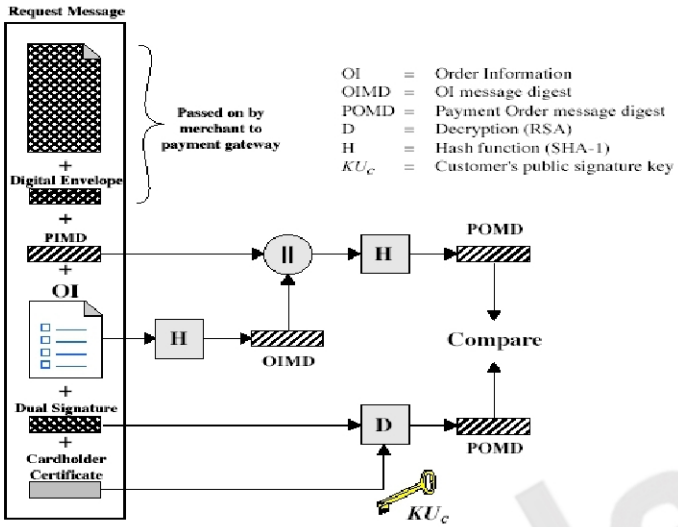


Purchase Response

- After receiving Purchase Request message merchant performs

- Verifies the cardholder certificate
- Verifies the dual signature
- Processes the order and forwards PI to the payment gateway
- Send purchase response to the cardholder

Purchase Request – Merchant



- Purchase Response message includes

  - order details and transaction number

  - message is signed with the merchants private key

  - signed message is send along with merchants certificate

- Customer verifies the certificate and the signature and takes action based on the response

Payment Authorization

- It ensures that the transaction was approved by the issuer
- Happens when merchant send payment details to payment gateway
- It guarantees that the merchant will receive payment and provide service
- Payment Authorization exchange consist of two messages

  1. Authorization Request
  2. Authorization Response

Authorization Request

- Prepared by merchant and send to payment gateway
- It consists of

    1. Purchase_related information
    2. Authorization_related information
    3. Certificates

Purchase-related information

- It was obtained from the customer
- It consists of
- - PI
  - The dual signature
  - The OI message digest
  - The digital envelope

Authorization-related information

- This information is generated by merchant
- It consists of

  - transaction ID (signed with merchant's private key, encrypted using one time key)
  - digital envelope (key encrypted with gateways public key)

Certificates

- The merchant sends to payment gateway

  - cardholder's certificate
  - Merchant's certificate

Authorization Response

- After getting authorization from the issuer, the payment gateway returns an authorization response message to the merchant
- It includes

    1. Authorization-related information
    2. Capture token information

3. Certificates

Authorization-related information

- It includes

  1. authorization block(signed with gateways private key, encrypted using one time key)

  2. Digital Envelope (key signed with

     merchants public key)

Capture token information

- used to effect payment later
- not processed by the merchant
- It is returned with a payment request later

Certificates

- The gateway's certificate is also included in message

Payment capture

- For obtaining payment merchant engage payment gateway in this transaction
- It consists of

  1. Capture Request message

  2. Capture Response message

Capture Request message

- merchant generates capture request block
- Block contains

  - amount to be paid

  - transaction id

- Block is signed and encrypted
- It also includes

  -capture token received earlier

- merchant's certificate

Capture Response message

- Payment gateway generates capture response block
- Block is signed and encrypted by payment gateway
- Also contains payment gateway's digital certificate

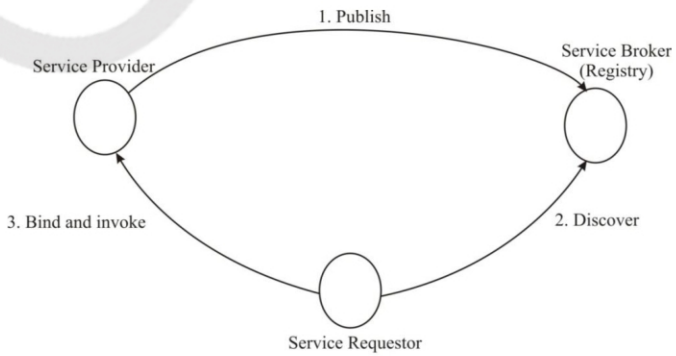
5. Explain Web Service Security and various standards used

- According to W3C(World-wide Web Consortium), a web service is defined as " A software system identified by a URI whose public interfaces and bindings are defined and described using XML."
- Its definition can be discovered by other software systems.
- These systems may then interact with the web service in a manner prescribed by its definition using XML based messages conveyed by Internet protocols

Entities involved

- An atomic web service involves three entities

1. requestor(client)
2. provider(server)
3. registry
   - Providers register or publish their services in a public registry
   - Requestors discover services by querying the registry for services that much match certain criteria.
   - Once a requester has identified a producer , it binds to and invokes the service of that provider



Technologies for web services

- Includes

1. XML
2. SOAP
3. WSDL and UDDI

XML

- A markup language uses tags as a mechanism to identify structures in a document or to specify presentation style/format
- Commonly used markup language is HTML.
- HTML have predefined tag sets
- Instead XML is a meta language, it provides facility to define tag sets

Example

```
<purchaseorder order date= "2009-01-05">
    <shipto country="India">
        <name> xyz  </name>
            <street> abbbc  </street>
    </shipto>
    <items>
            <item partnum =" 1223">
            <product name> x</ product name >
                    <quantity> 1</ quantity >
                    <unitprice> x</ unitprice >
        </items>
</purchaseorder>
```

- Start tag of an element - <>
- End tag - </>
- An element may contain data, and sub elements also
- Eg: shipto contains sub elements name,street etc

- An element may contain zero or more attributes also
- Eg: <shipto country="India"> contains single attribute ie "country"and value of that attribute is "India"

SOAP

- Simple Object Access Protocol
- It is a framework for exchanging structured information over the internet
- It defines one way message transfer between two entities
- SOAP message is an XML document made up of an envelope, which includes an optional header and a mandatory body.
- Most of the message information is contained in the body
- Header is used to extend the message and to include security information such as encryption algorithm used, digital signature computed etc.
- Body of SOAP message may contain Remote Procedure Calls in XML format
- SOAP contains request message and response message
- SOAP binding : the mapping between SOAP message and an underlying transport protocol

WSDL and UDDI

- Web Service Definition Language
- Is a language for describing web services
- It includes definition of various elements such as types, messages, operations, port types and bindings
- Port type - specifies one or more operations within its scope
- Operation – is an definition of an action. It involves one or more messages.
- Message – is a definition of data being exchanged as a part of an operation. Message have multiple parts, each part has a type
- Bindings – WSDL permits the web service developer to indicate the specific communication protocol to be used in support of each operation.

  < message name="message1">

  <part name=" "type=" "/>

  </message>

  < portType name="portType1">

```
<operation name="  ">
    <input message="message1"/>
</operation>
</portType>
```

UDDI

- Universal description, discovery and integration
- Is a registry that allows business across the globe to list themselves on the internet
- Client discover web services by querying the registry for specific services using SOAP messages.
- In response, they are provided access to the WSDL that describes the operations, messages and protocols for the desired web services
- The registry includes equivalent of white, green and yellow pages of telephone directory
- White page – provides address and contact information of a services that
- Yellow page – provides industrial categorization of service
- Green page – information about the service that business expose

Web Services Security Standards

WS-Security

- It is also known as WS-Sec.
- The main functions are
  1. To define the XML elements that are used to communicate security tokens
  2. defines the syntax and processing rules used to encrypt
  3. Defines the syntax and processing rules to create and represent a digital signature
- The first version was created by Organization for the Advancement of Structured Information Standards(OASIS) in 2004 with inputs from IBM, Microsoft and Verisign.
- Latest version, version 1.1 was released in February 2006.
- Security related information is contained within a <security> element in a SOAP header
- It specifies what operations are performed and in what order

- The <security> elements includes security tokens, keys, signatures, security meta information etc.
- Security claim : a statement made about subject's identity, privilege etc.
- Claim may be made by the subject himself or by another party on behalf of the subject.
- Claims are represented by security tokens
- Common examples of security tokens : user name+ password, Kerberos ticket
- Security tokens contains user name as pure text
- If binary data is there as signature or keys, then binary security token element is used

XML Encryption

- XML encryption standard was developed by W3C in 2002.
- It defines XML elements for representing encrypted data and keys used for encryption.
- It allows encryption at different levels
- <encrypted data> element is used to represent encrypted data in SOAP message
- Cipher text is enclosed in <cipher value>
- <KeyInfo> element identifies the key used

XML Digital Signature

- XML signature standard was developed by W3C and IETF(Internet Engineering Task Force) in 2002.
- Specifies the syntax for signatures and signature keys
- First step in generating signature is canonicalization
- It guarantees that syntactically identical documents produce the same serialized representations
- Signatures are involved in <signature> element of the SOAP message
- The major elements and sub elements involved are

1. <SignedInfo> - information about canonization and digital signature algorithm
2. <SignatureValue> - contains digital signature
3. <KeyInfo> - reference to key material needed to verify signature

Security Assertion Markup Language (SAML)

- Developed in May 2002 by OASIS
- It provides XML schema for expressing assertions about a principal.
- designed to support single sign-on and propagate authorization information
- SAML defines three types of assertions

Authentication

Attribute

Authorization

- Authentication: is an assertion by identity provider that it did authenticate a principal, using a particular authentication method at a particular time
- Attribute: is an assertion by identity provider that the value of particular attribute A for principal C is "a"
- Authorization: is an assertion by identity provider that a principal is permitted to perform a particular action on a particular resource

WS-Trust

- Two end points of a web service may have never interacted with each other.
- To build a trust between themselves, they could use an intermediary known to both parties
- WS-Trust is a proposal that enables security token interoperability by defining a request/response protocol by which SOAP actors can request of some trusted authority that a particular security token be exchanged for another.

WS-SecurityPolicy

- It enables a web service to specify the security tokens it will accept for authentication and access control
- It conveys information about which encryption algorithm to be used, which part has to be encrypted etc.
- These assertions are communicated as a part of WSDL or may be included in UDDI

6. Explain IDS and its types in detail

- An ID is a system designed to test/analyze network system traffic/events against a given set of parameters and alert/capture data when these thresholds are met.

- IDS uses collected information and predefined knowledge-based system to reason about the possibility of an intrusion.
- IDS also provide services like giving alarms, activating programs to try to deal with intrusion.

It performs three tasks

- It monitors "events of interest" occurring in the target system or in the network.
- It generates large amount of that which is then analyzed and converted into valuable information to be used by system administrator
- It creates a database of "interesting events". It raises an alert each time it observes any such events

Functions of IDS

- An IDS detects attacks as soon as possible and takes appropriate action.
- An IDS does not usually take preventive measures.
- It is a reactive rather than a pro-active agent.
- It plays a role of informant rather than a police officer.

Components of IDS

There are three components in an IDS:-

- Sensor: Responsible for capturing packets and sending to the Console class. Mainly used for detecting hacking
- Front end: provides direct user interface and setup IDIS configuration and update sensors and other parts of IDS
- Backend: provides database for recording information and alerting machine also. Based on recording information it create alerts and send to console/ front end

Types of Intrusion Detection System

Based on the functionality and architecture, IDSs may be classified into

- Host-base IDSs
- Network-based IDSs
- Anomaly based IDS
- Signature based IDs
- Distributed IDS

- Host-based IDSs
  - Detect attacks against a single host
  - Is implemented in the software
  - Resides on the top of host's operating system
  - Monitors the internal behavior of the host
  - Keep track of the modified files and file attributes

- Network-Based IDSs
  - Use network traffic as the audit data source
  - Detect attacks from network.
  - Captures information about packets flowing through the network

- Distributed IDS
  - capable of collecting information from multiple hosts and from network that connects to host also.
  - useful for analyzing multiple hosts

- Anomaly based IDS
  - records the normal behavior of a user
  - determination is done when the behavior of the system departures from normal
  - absence of normal behavior is monitored

- Signature based IDs
  - identify specific patterns or events of an attacker
  - each such pattern is called a signature
  - maintains a database of signatures
  - if a match is observed with database, then alert is given
  - presence of specific signature is monitored

7. Explain DdoS attack with prevention and detection and how to defense against DoS attacks

- In a **DDoS attack**, the incoming traffic flooding the victim originates from many different sources.
- is an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource.
- The number of requests coming to the target system shut downs it forcefully.
- This prevents authorize users from using the system
- It is done through distributed network.

DDoS Prevention

- **Preventive measures at the victim side**

- One way of handling SYN attacks is to drop requests for TCP connection
- This can create problem if the victim is not able to distinguish between SYN packets from an attacker and a normal user

One way to handle issue is

- Categorize IP addresses as “almost certainly genuine”, “ probably spoofed” etc
- under moderate load, all incoming packets are entertained
- when heavy load, packets with unfamiliar source address are discarded

Another way

- under high load, allocate a full buffer of about 300 bytes for a given TCP connection request only upon completion of three way handshake protocol

- **Preventive measures inside the network**

- egress filtering
- Distribute Route Filtering

Egress filtering

- Let A be the set of all externally visible IP addresses within the network.
- Egress router examines the source address of each packet leaving it.
- If the address doesn’t match any address in A, it drops the packet

Distribute Route Filtering

- A router is used for filtering packets with spoofed address
- It uses packets source address to make decision
- To implement DRP, filter maintains set of source address from which packets arrive to some destination
- If a packet with source IP address arrives via an interface that it should not have, that packet is discarded

DDoS Detection

- Another approach to handle DDoS is to detect it and take remedial action

- In a TCP connection, we are having SYN packets and RST packets

  SYN – TCP connection request packet

  FIN – TCP connection termination packet

  RST – connection abort

- To construct an anomaly detection system, we define some variables

  S_i = SYN packets arrives in the i^{th} interval

  F_i = FIN packet arrives in the i^{th} interval

  D_i = normalized difference between SYN and

  FYN packets in the i^{th} interval

  ie, $D_i = S_i - F_i / F_i$

  T = threshold for detection

- To construct an anomaly detection system, we define some variables

  S_i = SYN packets arrives in the i^{th} interval

  F_i = FIN packet arrives in the i^{th} interval

  D_i = normalized difference between SYN and

  FYN packets in the i^{th} interval

  ie, $D_i = S_i - F_i / F_i$

  ^{T} = threshold for detection

- It is observed for different time series
- Different algorithms are used to detect attacks by monitoring the above series

Algorithm 1

- Raise an alert if the most recently computed detection variable D_i exceeds the threshold
- Problem
  - may raise false alarms since decisions is based on point values
  - if cumulative value go beyond threshold , it won't raise an alarm

Algorithm 2

- raise an alert if the "smoothed average" of previous D value exceeds threshold

- The smoothed average value, A_i is calculated as

$$A_i = \alpha D_i + (1-\alpha) A_{i-1}$$

Where

$$0 < \alpha < 1 \text{ and } A_0 = 0$$

Algorithm 3

- Define a modified cumulative sum of previous values of D.
- raise an alert if this value exceeds the threshold

IP traceback

- Usually source address is spoofed address
- So we attempt to identify the path traversed by the attack packets
- Two approaches

- Packet marking

- Packet logging

Packet marking

- Packets keep track of the routers it has visited

Packet logging

- Each router keeps track of the packets passing through it

Defenses against DoS

- It is important to recognize these attacks
- cannot be prevented entirely.
- Can be deliberate or accidentally(eg: high publicity about a specific site)

There are four lines of defense against DDoS attacks

1. Attack prevention and preemption (before the attack)

2. Attack detection and filtering (during the attack)

3. Attack source traceback and identification (during and after the attack)

4. Attack reaction (after the attack)

Attack prevention and preemption

- This mechanism enables the victim to tolerate attack attempts without denying service to legitimate clients.
- Done before the attack
- Techniques include

- enforcing policies for resource consumption

- providing backup resources

- Most recommended option

- limit the ability of systems to send packets with spoofed source addresses

- ISP can use reverse path filter can help identify some such packets
- In that case, the path from the ISP to the spoofed address differs to that used by the packet to reach the ISP
- Next alternative is *selective drop or random drop*

- System's TCP/IP network code can be modified to selectively drop an entry for an incomplete connection from the TCP connections table when it overflows

- as a result a new connection attempt is proceeded.

- This is known as *selective drop or random drop*

Attack detection and filtering

- Done during the attack
- Attempts to detect the attack as it begin and respond immediately.
- This minimizes the impact of the attack on the target.
- Detection involves looking for suspicious patterns of behavior.
- Response involves filtering out packets likely to be part of the attack.

Attack source traceback and identification

- Done during and after the attack
- Attempt to identify the source of the attack as a first step in preventing future attacks.

- Is not fast enough to mitigate an ongoing attack.

Attack reaction

- Done after the attack
- is an attempt to eliminate the effects of an attack.

8. Explain Malware Detection

What is a malware ?

- A Malware is a set of instructions that run on your computer and make your system do something that an attacker wants it to do.

Is used for

- Steal personal information
- Delete files
- Click fraud
- Steal software serial numbers
- **malware** is a broad term used to describe all sorts of unwanted or malicious code.
- **Malware** can include viruses, spyware, adware, nagware, trojans, worms, and more.

What is a Virus ?

- **Viruses** are a specific type of **malware**
- *a program that can infect other programs by modifying them to include a, possibly evolved, version of itself*
- Types of viruses includes

  Polymorphic

  Methamorpic
- Metamorphic malware is rewritten with each iteration so that each succeeding version of the code is different from the preceding one.
- The code changes makes it difficult for signature-based antivirus software programs to recognize
- Polymorphic malware also makes changes to code to avoid detection.
- It has two parts, but one part remains the same with each iteration, which makes the malware a little easier to identify.

- Eg: polymorphic virus might have a virus decryption routine (VDR) and an encrypted virus program body (EVB).
- When an infected application launches, the VDR decrypts the encrypted virus body back to its original form so the virus can perform its intended function.
- Once executed, the virus is re-encrypted and added to another vulnerable host application..

Malware detection

- **Worm**

- most commonly known form of malware

- they, by themselves, do not do any damage to any computers

- worm is only meant to move around to as many computers as possible without altering any functionality.

- Worm Detection

- Various challenges are involved in worm detection

  1. speed
  2. Non- monomorphic worms
  3. Zero-hour worms

- Characteristics that an IDS should have

1. Monomorphic worm instances share common substrings
2. A particular worm targets one vulnerable application
3. Scanning techniques employed by the worms

- Worm Signature Extraction

- to do worm detection , we have to identify worm signature ie, patterns of substrings

- packets from “never-seen-before” IP address is checked

- commonly occurring strings, which are the parts of protocols are considered

- Such strings are included in a white list

- Contents of white list are considered as genuine

- Another technique is using “Rabin fingerprints”
- It identifies the common substrings in different packets
- In this message is divided in to blocks and hash value of the block is computed
- To identify a worm, a table T is created, which has four columns
- The columns are

    - destination port address(port#)

    - Rabin Fingerprint Value (RF)

    - prevalence count (PC)

    - set of IP source- destination pairs (IP)

- For each incoming packet, the RF value is calculated for each block
- Each block is checked against white list
- If in white list, ignored
- For each block passing, entry is made in T
- If a fingerprint comes for the first time, a new entry is made in the table
- The port# and RF value is initialized
- PC is set to 1 and IP to null
- If both port number and finger print encountered for a previous packet, no new row is created
- Only PC value will be incremented
- If the PC count exceeds a given threshold, IDS suspects a worm has been unleashed
- Then it will start tracking the source –destination pairs of packets carrying such strings
- Then one more column is added to enter source-destination IP address pair
- If the address – dispersion column exceeds a threshold, then it conclude that there is a strong likelihood of occurrence of worm

Virus detection

- anti viruses are used

- virus scanners attempt to detect and identify malicious executables in files and emails

- then they create and update database of virus signatures

9. Explain database access control in detail

Database Access Control

- Commercial and open-source DBMSs typically provide an access control capability for the database.
- The DBMS operates on the assumption that the computer system has authenticated each user.
- For users who are authenticated and granted access to the database, a database access control system provides a specific capability that controls access to portions of the database.

- DBMS can support a range of administrative policies

1. **Centralized administration:** A small number of privileged users may grant and revoke access rights.
2. **Ownership-based administration:** The owner (creator) of a table may grant and revoke access rights to the table.
3. **Decentralized administration:** In addition to granting and revoking access rights to a table, the owner of the table may grant and revoke authorization rights to other users, allowing them to grant and revoke access rights to the table.

SQL-Based Access Definition

- SQL provides two commands for managing access rights,

  - GRANT and REVOKE.

- Grant command can be used to grant one or more access rights or can be used

to assign a user to a role

GRANT { privileges | role }

[ON table]

TO { user | role | PUBLIC }

[IDENTIFIED BY password]

[WITH GRANT OPTION]

- Example

GRANT SELECT ON ANY TABLE TO ALICE

This statement enables user to query any table in the database.

⦿ Different implementations of SQL provide different ranges of access rights.

• Select: Grantee may read entire database; individual tables; or specific columns in a table.

• Insert: Grantee may insert rows in a table; or insert rows with values for specific columns in a table.

• Update: Semantics is similar to INSERT

• Delete: Grantee may delete rows from a table.

• References: Grantee is allowed to define foreign keys in another table that refer to the specified columns.

⦿ The REVOKE command has the following syntax:

REVOKE { privileges | role }

[ON table]

FROM { user | role | PUBLIC }

⦿ Thus, the following statement revokes the access rights of the preceding example:

⦿ REVOKE SELECT ON ANY TABLE FROM ALICE

Cascading Authorizations

⦿ The grant option enables an access right to cascade through a number of users.

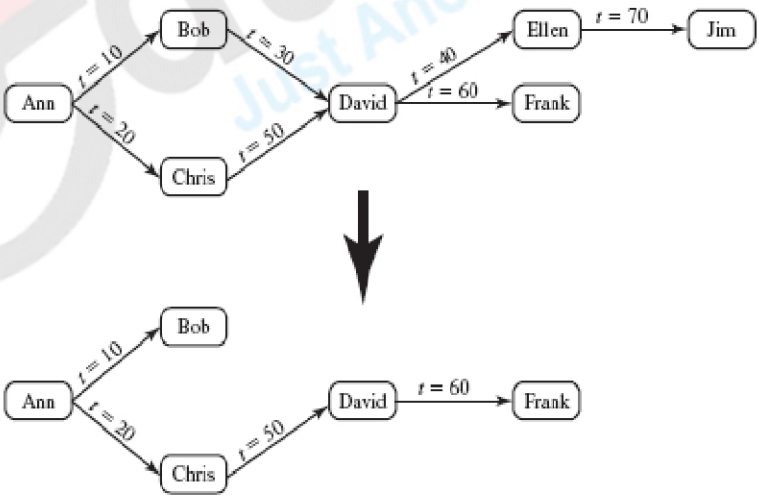


Figure 5.4 **Bob Revokes Privilege from David**

- Just as the granting of privileges cascades the revocation of privileges also cascaded.

Role-Based Access Control (RBAC)

- RBAC is a natural fit for database access control.
- database system often supports dozens of applications
- an individual user may use a variety of applications to perform a variety of tasks, each of which requires its own set of privileges.
- We cannot grant users all of the access rights they require for all the tasks they perform.
- RBAC provides a means of easing the administrative burden and improving security.
- we can classify database users in three broad categories:
  • **Application owner:** An end user who owns database objects (tables, columns, rows) as part of an application.
- **End user other than application owner:** An end user who operates on database objects via a particular application but does not own any of the database objects.
- **Administrator:** User who has administrative responsibility for part or all of the database.

- An application has associated with it a number of tasks, with each task requiring specific access rights
- For each task, one or more roles can be defined that specify the needed access rights.
- The application owner may assign roles to end users.
- Administrators are responsible for more sensitive roles, including those having to do with managing data files, users, and security mechanisms.
- A database RBAC facility needs to provide the following capabilities:
  - Create and delete roles.
  - Define permissions for a role.
  - Assign and cancel assignment of users to roles.

- Example of the use of roles in database security is the RBAC facility provided by Microsoft SQL Server.
- SQL Server supports three types of roles:
  - server roles
  - database roles
  - user-defined roles

  The first two types of roles are referred to as fixed role
  They are preconfigured for a system with specific access rights.

10. Explain inference in detail

- process of performing authorized queries and deducing unauthorized information from the legitimate responses received

- The attacker may make use of non sensitive data as well as metadata.

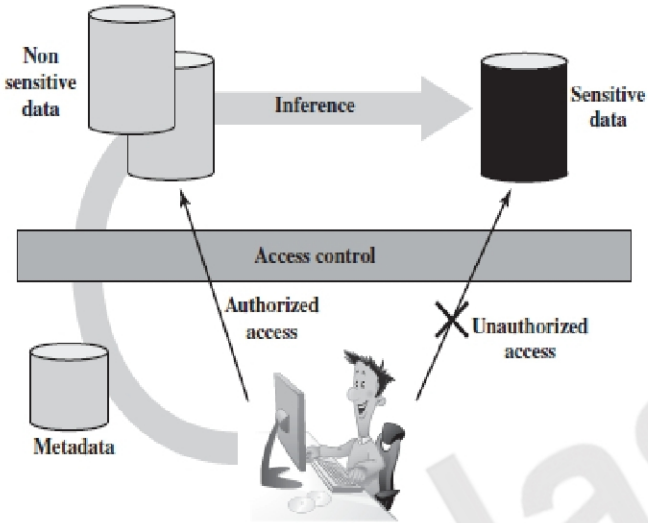


Figure 5.5 **Indirect Information Access via Inference Channel**

- Metadata - knowledge about correlations or dependencies among data items that can be used to deduce information not otherwise available to a particular user.
- Inference channel - the information transfer path by which unauthorized data is obtained
- Two inference techniques can be used

1. analyzing functional dependencies between attributes within a table or across tables

2. merging views with the same constraints

Item	Availability	Cost ($)	Department
Shelf support	in-store/online	7.99	hardware
Lid support	online only	5.49	hardware
Decorative chain	in-store/online	104.99	hardware
Cake pan	online only	12.99	housewares
Shower/tub cleaner	in-store/online	11.99	housewares
Rolling pin	in-store/online	10.99	housewares

(a) Inventory table

Availability	Cost ($)
in-store/online	7.99
online only	5.49
in-store/online	104.99

Item	Department
Shelf support	hardware
Lid support	hardware
Decorative chain	hardware

(b) Two views

Item	Availability	Cost ($)	Department
Shelf support	in-store/online	7.99	hardware
Lid support	online only	5.49	hardware
Decorative chain	in-store/online	104.99	hardware

(c) Table derived from combining query answers

Figure 5.6 **Inference Example**

- Two approaches to dealing with the threat of disclosure by inference:

1. Inference detection during database design
2. Inference detection at query time

Inference detection during database design

- This approach removes an inference channel by altering the database structure or by changing the access control rule to prevent inference.
- Example:

- removing data dependencies

- using more fine-grained access control roles in an RBAC scheme.

Inference detection at query time

- This approach seeks to eliminate an inference channel violation during a query or series of queries.
- If an inference channel is detected, the query is denied or altered.