Distributed Systems
Delhi Technological University
Security

Divyashikha Sethia
divyashikha@dtu.ac.in

Objectives

- ➢Security Management

i. Communication between users or processes
  - secure channel
  - authentication
  - message integrity
  - confidentiality

ii. Authorization for access control

- ➢Management of Cryptographic Keys

Security Threats, Policies, and Mechanisms

- Dependability includes:
  availability, reliability, safety, and maintainability.

- Dependable computer system is one that we justifiably trust to deliver its services
  - **Confidentiality** – information disclosed only to authorized parties.
  - **Integrity** - alterations to a system's assets can be made only in an authorized way.

Security Threats, Policies, and Mechanisms…

Threats:

1. **Interception**: unauthorized party has gained access to a service or data,
   - overhearing of communication

2. **Interruption**: services or data become unavailable,
   - file is corrupted or lost
   - denial of service attacks,

3. **Modification**: unauthorized changing of data or tampering with a service so that it no longer adheres to its original specifications,
   - changing transmitted data tampering with database entries
   - changing a program

Data Falsification

4. **Fabrication**: additional data or activity are generated that would normally not exist,
   - Add an entry into a password file or database
   - replaying previously sent messages

Security Policy

Defines actions of entities that are allowed or prohibited.

Security mechanisms are:

1. **Encryption**: transforms data into something an attacker cannot understand (Data confidentiality, integrity)

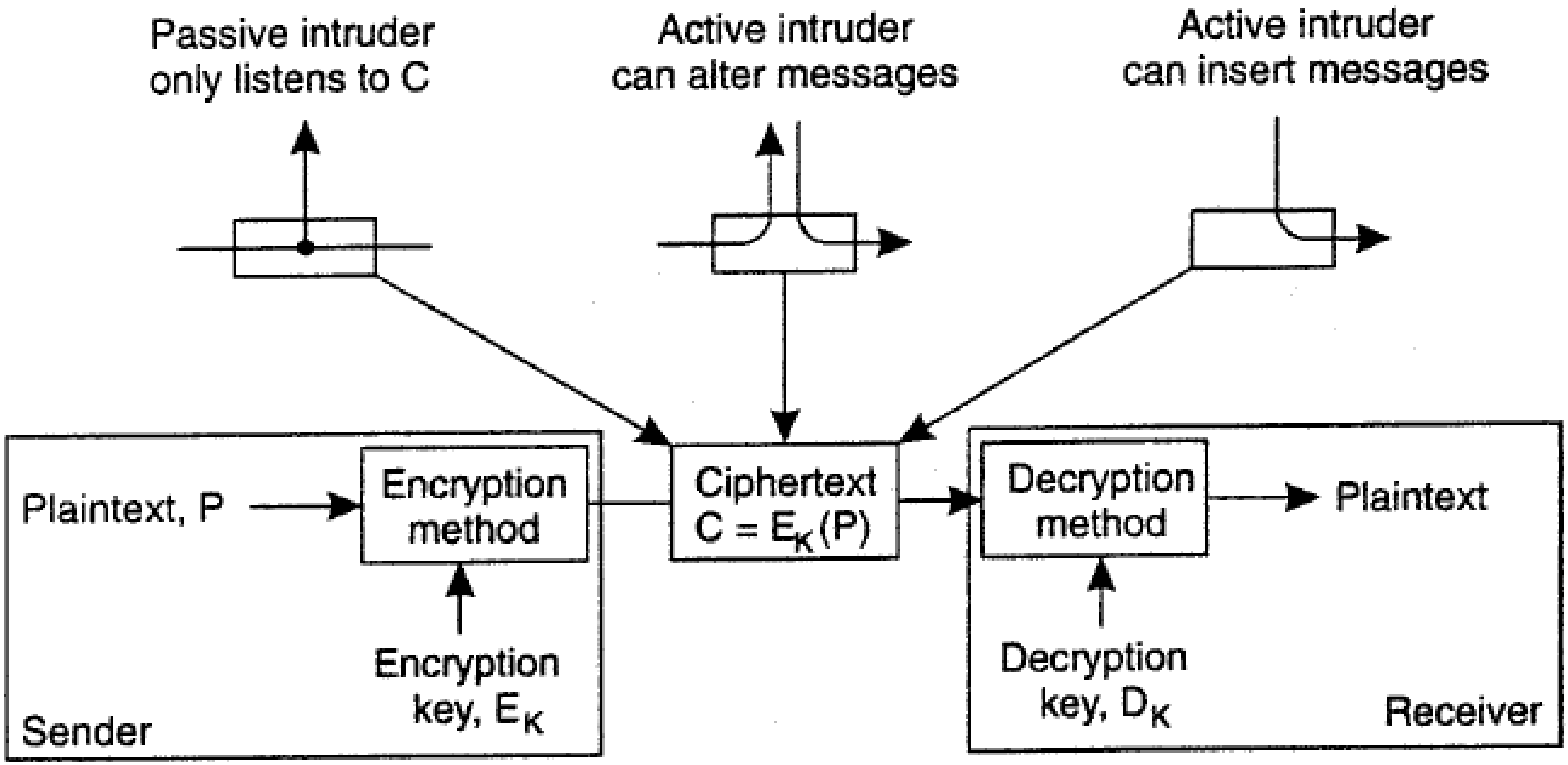
2. **Authentication** (identity of identifier)

3. **Authorization** (permission to access)

4. **Auditing** (trace which clients accessed what, and which way) – analysis of security breach

Cryptography

-



Hash functions

h = H (m)
-M arbitrary bytes, h is fixed length
one-way functions, meaning that it is computationally infeasible to find the input *m that corresponds to a known output h*

-m’ != m then H(m’) != H(m)

. Different types of failures.

Cryptography

- Symmetric - DES
- Asymmetric RSA
- Hash (MD5) (Self Study)

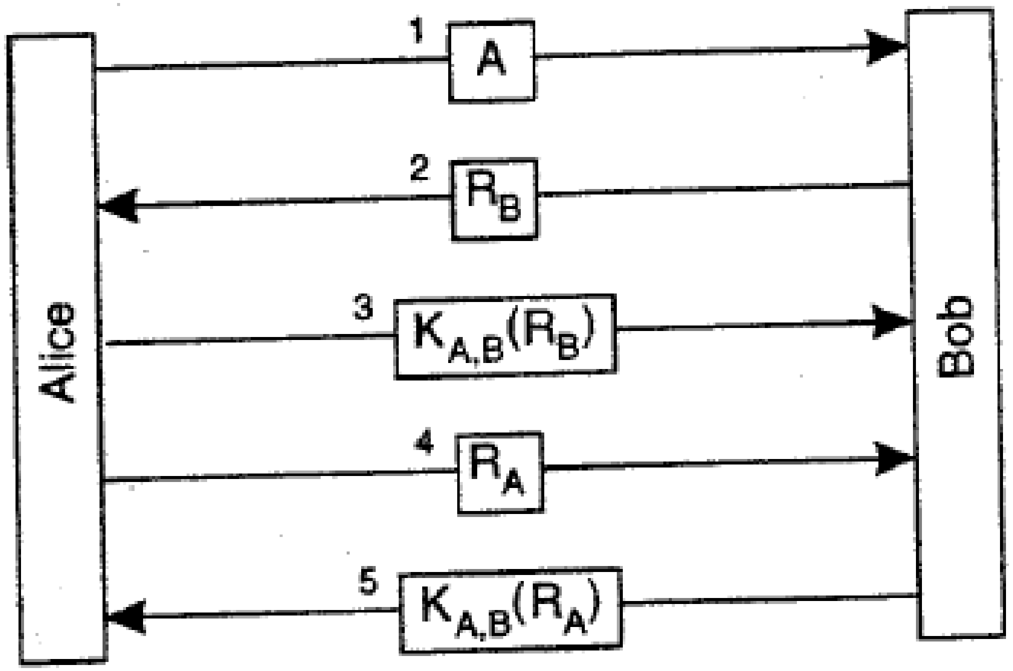
Secure Channels

A secure channel protects senders and receivers against -

- interception (confidentiality to prevent eavesdropping)
- modification (mutual authentication and message integrity)
- fabrication (mutual authentication and message integrity)

Authentication

Authentication Based on a Shared Secret Key



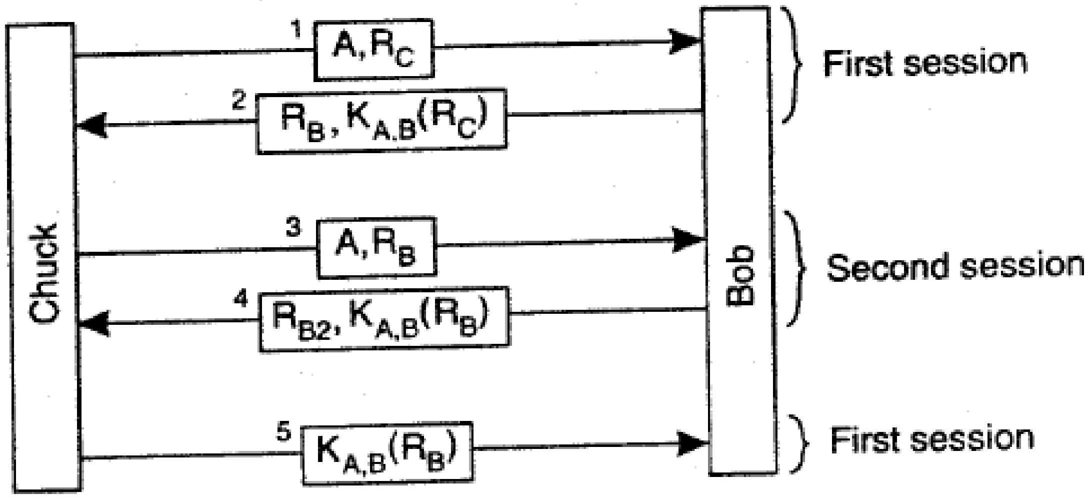
RA, RB: Challenges **(random number)**

Authentication

Reflection Attack: intruder called Chuck (C)

Chuck's goal is to set up a channel with Bob so that Bob believes he is talking to Alice

How to return $K_{A,B}(RB)$?



1. Alice's identity A, along with a challenge R_C
2. Bob returns his challenge R_B and the response $K_{A.B}(R_C)$
3. Chuck needs to send $K_{A,B}(R_B)$ – he does not know $K_{A,B}$!
4. sends A and R_B in a single message as before, but now pretends that he wants a second channel responds with $K_{A,B}(R_B)$ and another challenge R_{B2}
5. Chuck has $K_{A,B}$ (R_B) and finishes setting up the first session by returning message 5 containing the response $K_{A,B}(R_B)$,

Authentication

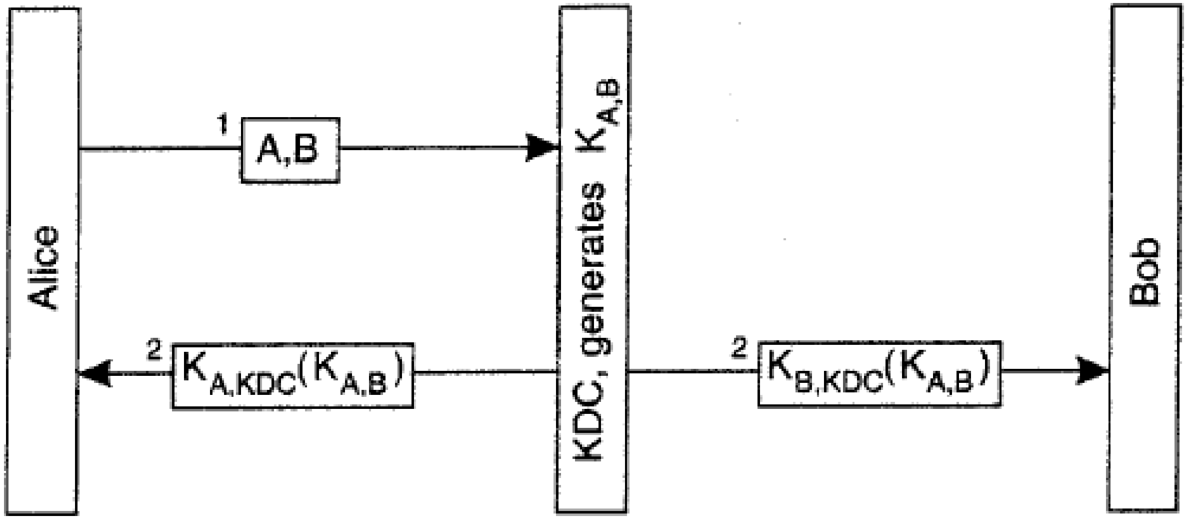
Solution: Use unique nonce

Prone to man in the middle attack

Authentication

Authentication Using a Key Distribution Center (KDC)

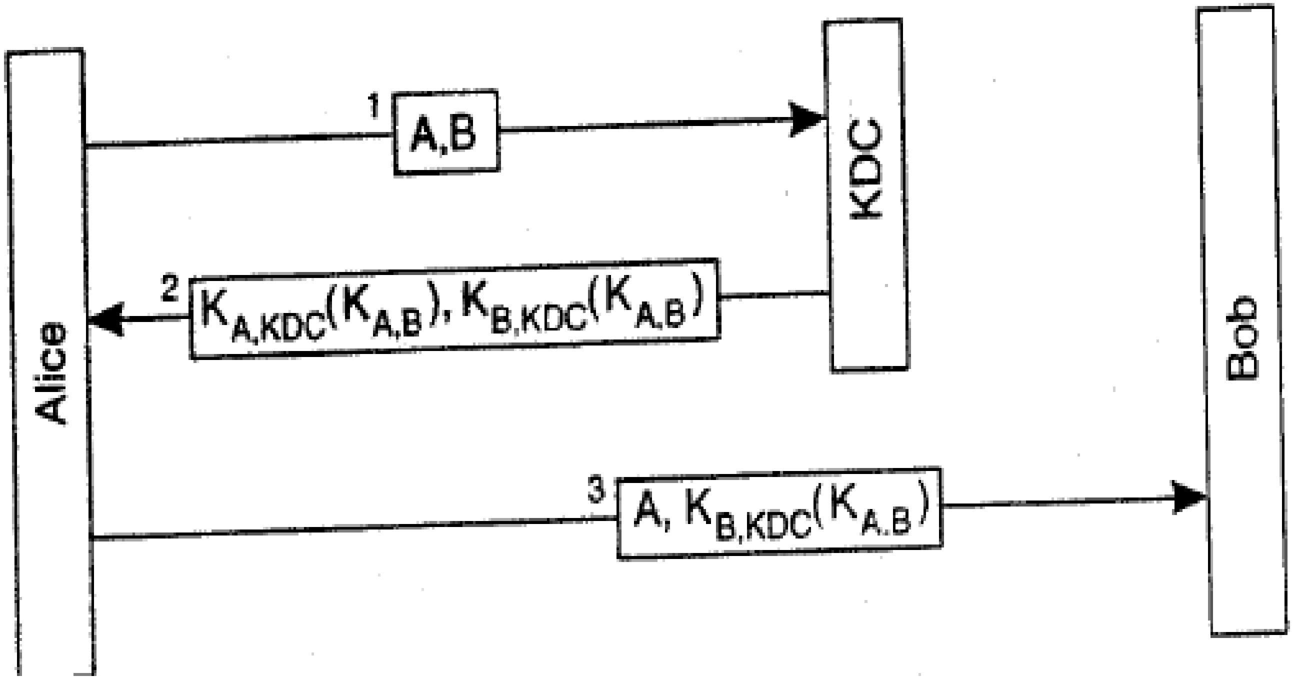
Maintaining secret with N hosts is not scalable



Drawbacks:
-Alice may want to start setting up a secure channel with Bob even before Bob had received the shared key from the KDC
- KDC in the loop can give Alice *($K_{B,KDC}(K_{A,B})$) (Ticket)*

Authentication

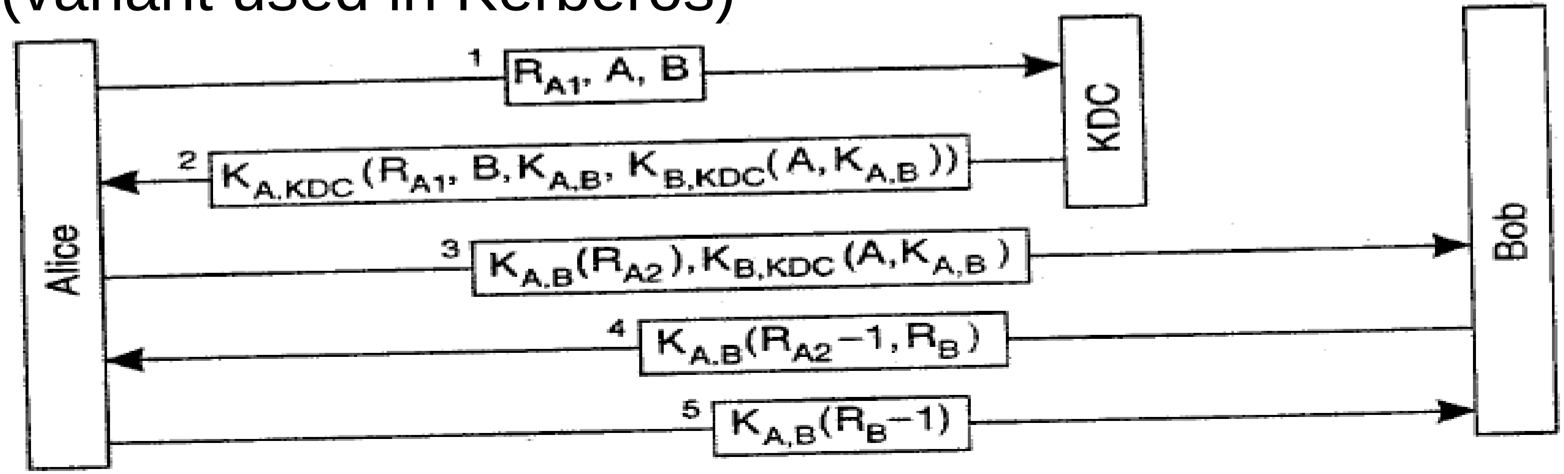
Using a ticket and letting Alice set up a connection to Bob.



Drawbacks:
- Chuck steals Bobs key $K_{B,KDC}$

Authentication

The Needham-Schroeder authentication protocol (variant used in Kerberos)

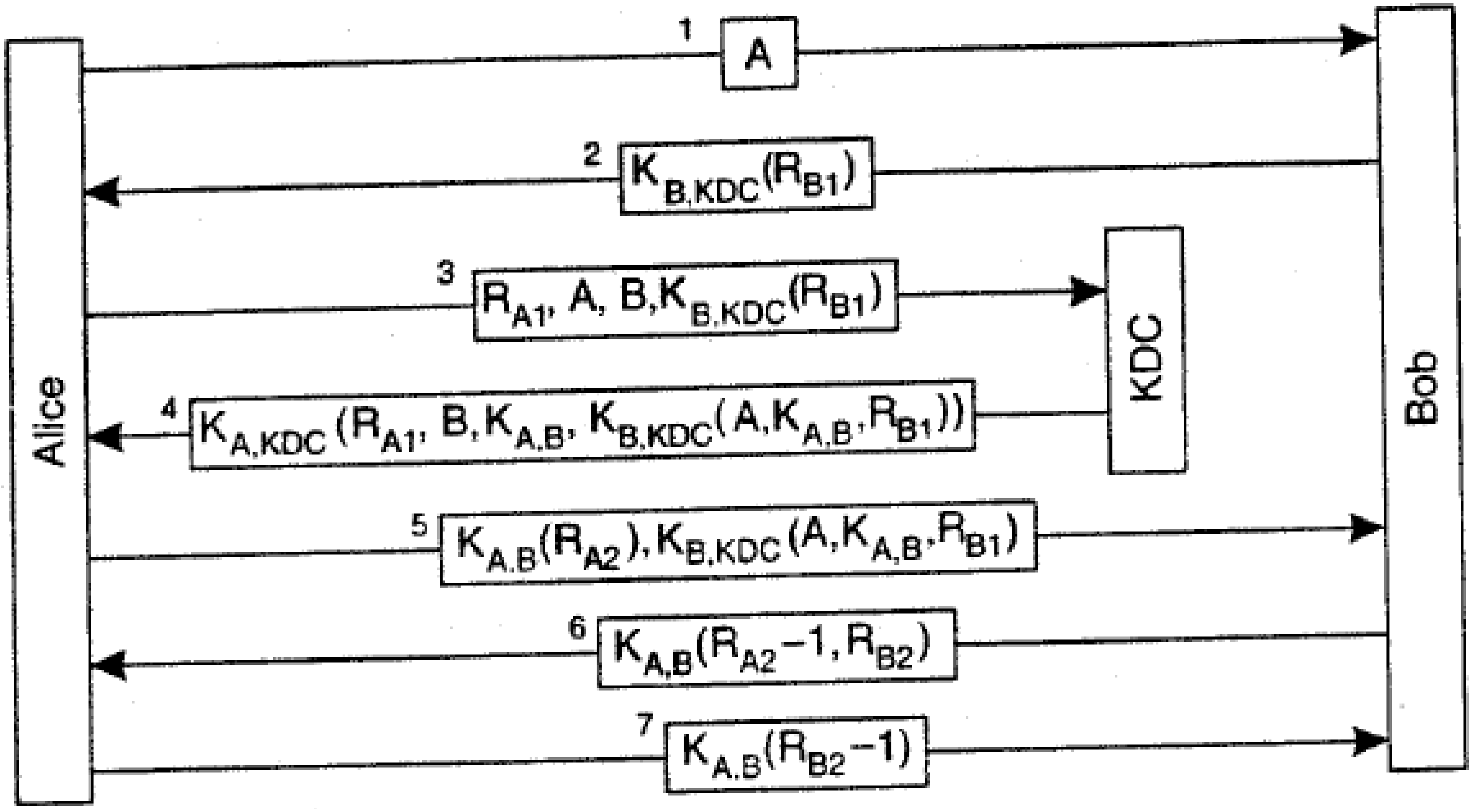

Alice
KDC
Bob
1
R_{A1}, A, B
2
$K_{A,KDC}(R_{A1}, B, K_{A,B}, K_{B,KDC}(A, K_{A,B}))$
3
$K_{A,B}(R_{A2}), K_{B,KDC}(A, K_{A,B})$
4
$K_{A,B}(R_{A2}-1, R_B)$
5
$K_{A,B}(R_B-1)$

challenge *R_{A1} that Alice sends to the KDC along with her request to set* up a channel to Bob is also known as a nonce. (random number that is used only once, such as one chosen from a very large set. The main purpose of a nonce is to uniquely relate two messages to each other, in this case message 1 and message 2 (replay of an older message)

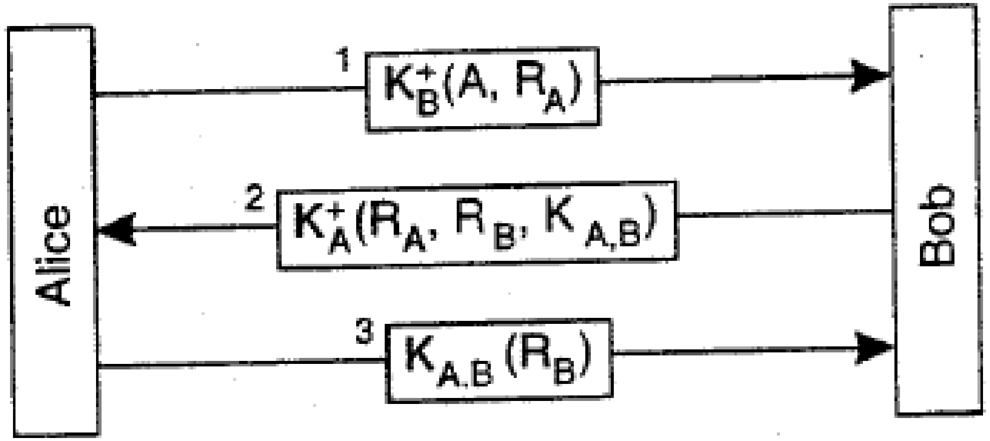
Drawback: replay message 3 and get Bob to set up a channel. Bob will then believe he is talking to Alice

Authentication

Protection against malicious reuse of a previously generated session key in the Needham-Schroeder protocol.


Alice
KDC
Bob
1 A
2 $K_{B,KDC}(R_{B1})$
3 R_{A1}, A, B, $K_{B,KDC}(R_{B1})$
4 $K_{A,KDC}(R_{A1}, B, K_{A,B}, K_{B,KDC}(A, K_{A,B}, R_{B1}))$
5 $K_{A,B}(R_{A2}), K_{B,KDC}(A, K_{A,B}, R_{B1})$
6 $K_{A,B}(R_{A2}-1, R_{B2})$
7 $K_{A,B}(R_{B2}-1)$

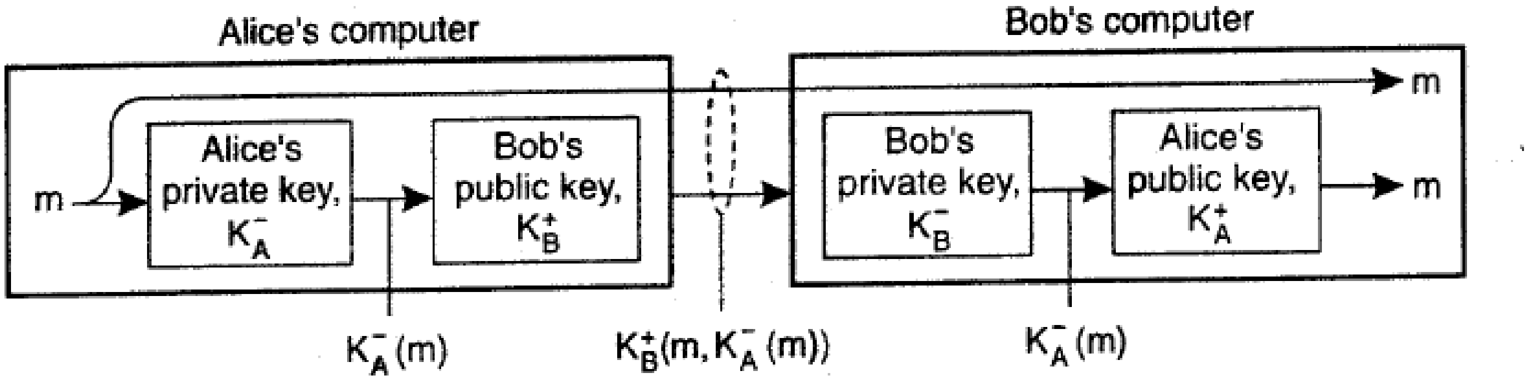
Authentication Using Public-Key Cryptography



Message Integrity and confidentiality

Message integrity means that messages are protected against surreptitious modification; confidentiality ensures that messages cannot be intercepted and read by eavesdroppers.

1. Digital Signatures: public-key cryptosystem such as RSA

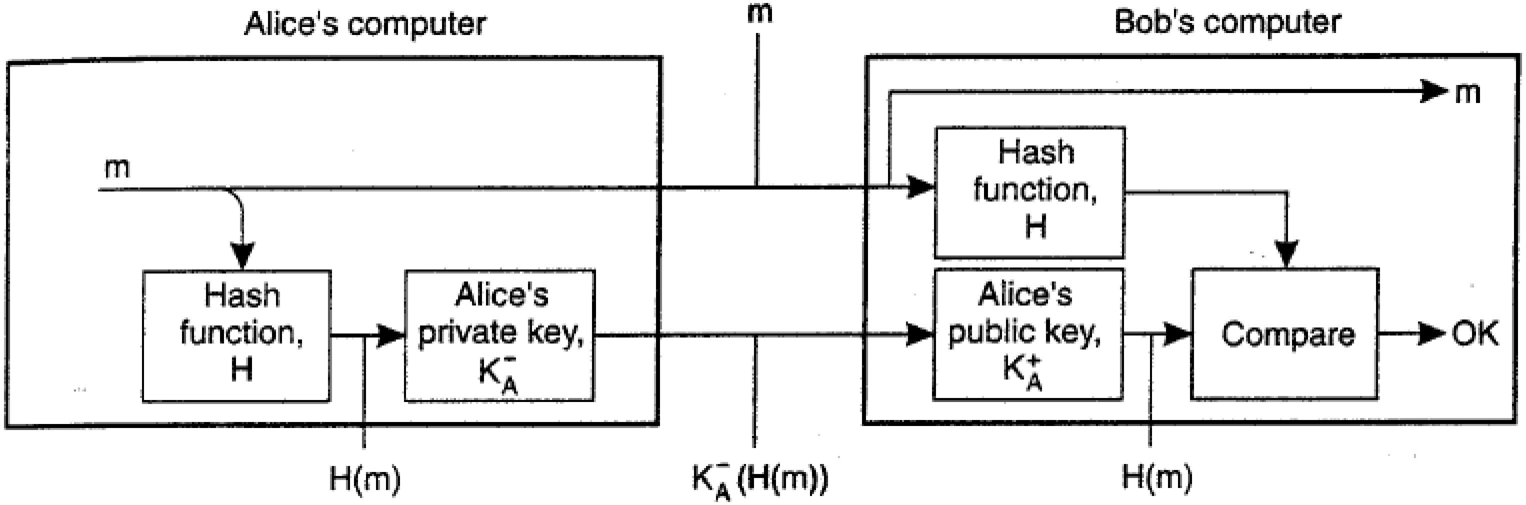


Alice's computer
Bob's computer
m
Alice's private key, K_A^-
Bob's public key, K_B^+
Bob's private key, K_B^-
Alice's public key, K_A^+
m
m
$K_A^-(m)$
$K_B^+(m, K_A^-(m))$
$K_A^-(m)$

Problems:

- validity of Alice's signature holds only as long as Alice's private key remains a secret
- Alice decides to change her private key
- Costly to encrypt entire message with private key

Message Integrity and confidentiality



Message Integrity and confidentiality

Session Keys

-After mutual authentication, the communicating parties generally use a unique shared session key for confidentiality:

-key is used often, it becomes easier to reveal it.

- protection against replay attacks

Authentication - Kerberos

Kerberos was developed at M.I.T. and is based on the Needham-Schroeder authentication protocol

Kerberos can be viewed as a security system that assists clients in setting up a secure channel with any server that is part of a distributed system.

Security is based on shared secret keys.

There are two different components.

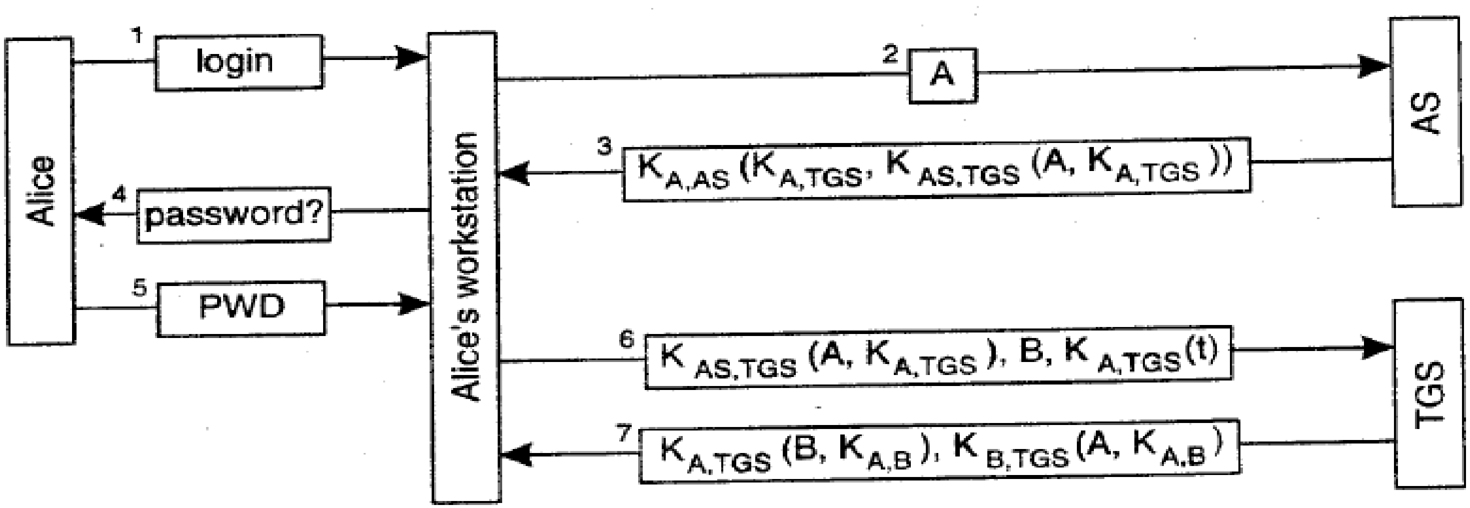
- The **Authentication Server (AS)** is responsible for handling a login request from a user. The AS authenticates a user and provides a key that can be used to set up secure channels with servers.

- **Ticket Granting Service (TGS)** Setting up secure channels is handled by a Ticket Granting Service (TGS).

TGS hands out special messages, known as tickets, that are used to convince a server that the client is really who he or she claims to be.

Kerberos

Alice logs onto a distributed system that uses Kerberos and how she can set up a secure channel with server Bob session key $K_{A,TGS}$ *and a ticket*



Alice
Alice's workstation
AS
TGS
1
login
2
A
3
$K_{A,AS}(K_{A,TGS}, K_{AS,TGS}(A, K_{A,TGS}))$
4
password?
5
PWD
6
$K_{AS,TGS}(A, K_{A,TGS}), B, K_{A,TGS}(t)$
7
$K_{A,TGS}(B, K_{A,B}), K_{B,TGS}(A, K_{A,B})$

ticket is encrypted with the secret key $K_{AS,TGS}$ shared between the AS and the TGS

Msg 1,2,3 – login name

Alice's password $K_{A,AS}$ is never sent as plaintext across the network, but also that the workstation does not even have to temporarily store it.

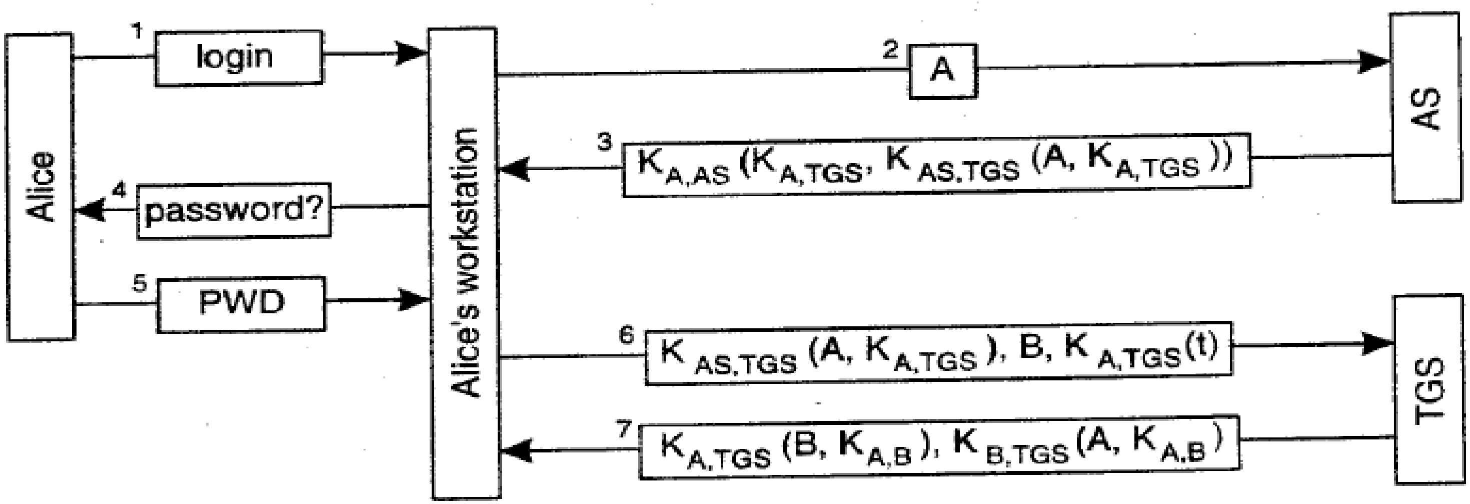
The ticket received from the AS is stored temporarily (typically for 8-24 hours), and will be used for accessing remote services.

to talk to Bob, she requests the TGS to generate a session key for Bob, shown as message 6

Proof of identity of Alice: $K_{AS,TGS}[A,K_{A,TGS}]$

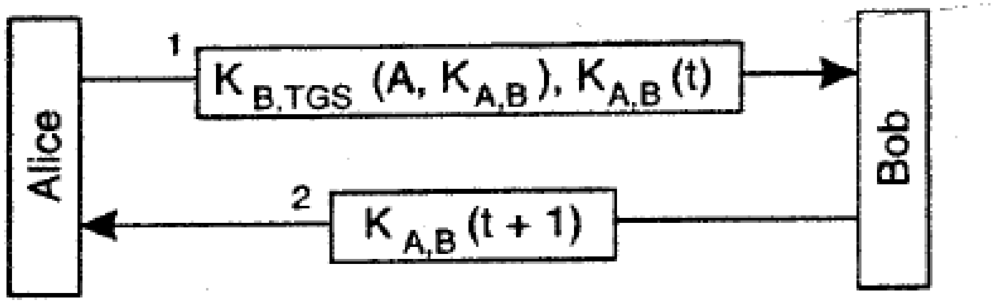
TGS responds with a session key $K_{A,B}$, again encapsulated in a ticket that Alice will later have to pass to Bob.

Kerberos


Alice
1
login
Alice's workstation
2
A
AS
3
$K_{A,AS}(K_{A,TGS}, K_{AS,TGS}(A, K_{A,TGS}))$
4
password?
5
PWD
6
$K_{AS,TGS}(A, K_{A,TGS}), B, K_{A,TGS}(t)$
TGS
7
$K_{A,TGS}(B, K_{A,B}), K_{B,TGS}(A, K_{A,B})$

Message 6 also contains a timestamp, *t, encrypted with the secret key shared* between Alice and the TGS. – maliciously replaying message 6 again single sign-on.
As long as Alice does not change workstations, there is no need for her to authenticate herself to any other server that is part of the distributed system AS and TGS responsible for Client authentication Servers expect a correct ticket from the client before proceeding the service

Kerberos



Alice sends to Bob a message containing the ticket she got from the TGS, along with an encrypted timestamp. When Bob decrypts the ticket he notices that Alice is talking to him, because only the TGS could have constructed the ticket.

Bob verifies timestamp t by the shared secret $K_{A,B}$ (assured talking to Alice and not a replay due the fact that key is tied with time)

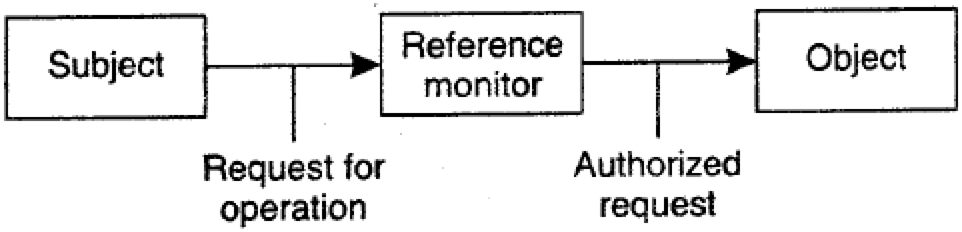
Msg 2: Assures Alice that it is sent by Bob

Access Control

Secure channel – access to resources.

access rights is referred to as access control

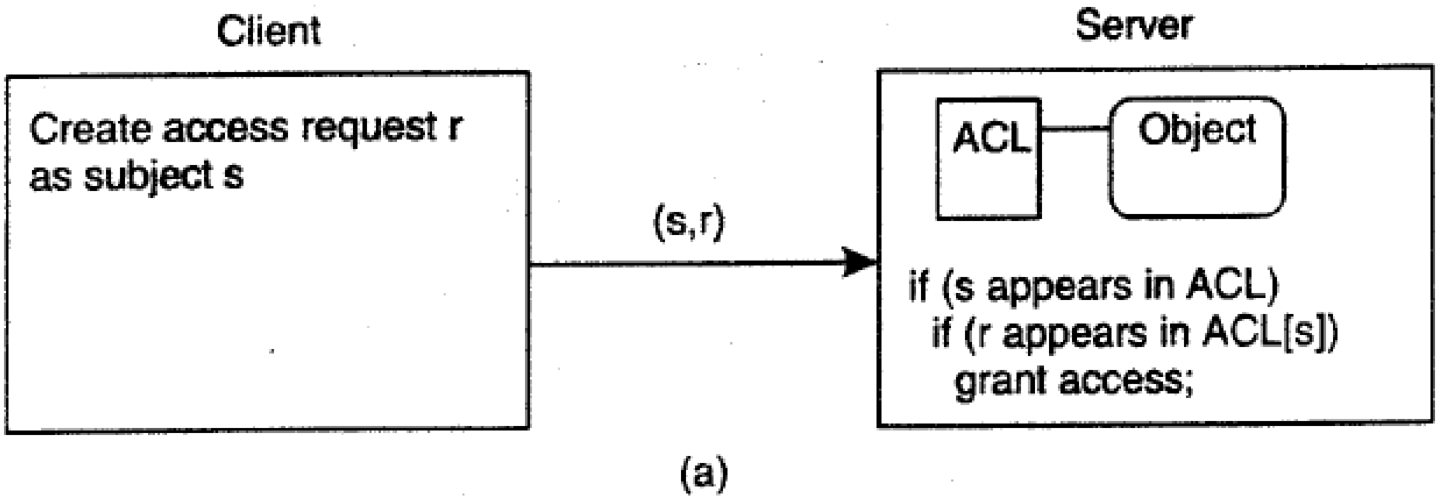
authorization is about granting access rights



General model of controlling access to objects

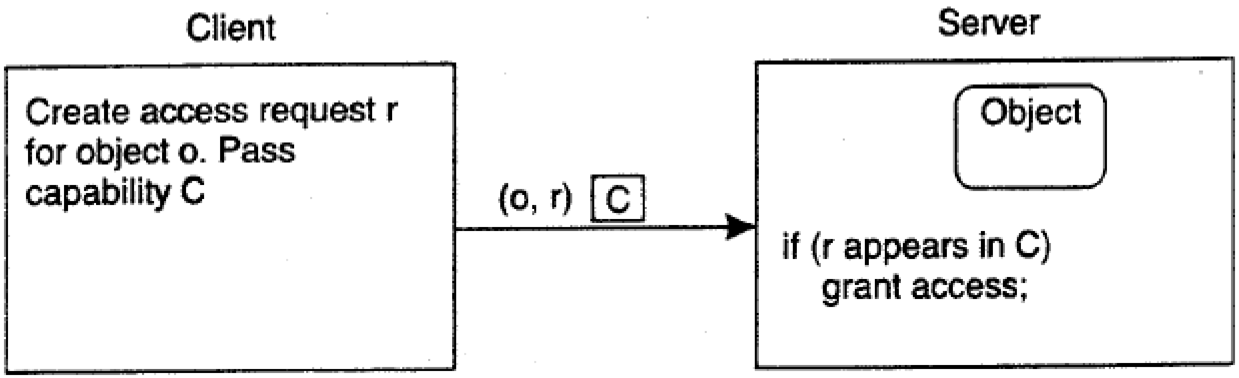
- Access Control Matrix
  - subject is represented by a row in this matrix; each object is represented by a column.
  - Many users – sparse matrix
  - each object maintain a list of the access rights of subjects that want to access the object: Access Control List(ACL)

Access Control



Access Control

- **Capabilities**:
  - each subject has a list of capabilities it has for each object (corresponds to entry in access control matrix
  - Capability compared to a ticket: its holder is given certain rights that are associated with that ticket.
  - Must be protected against modifications by its holder. – eg: protect (a list of) capabilities with a signature

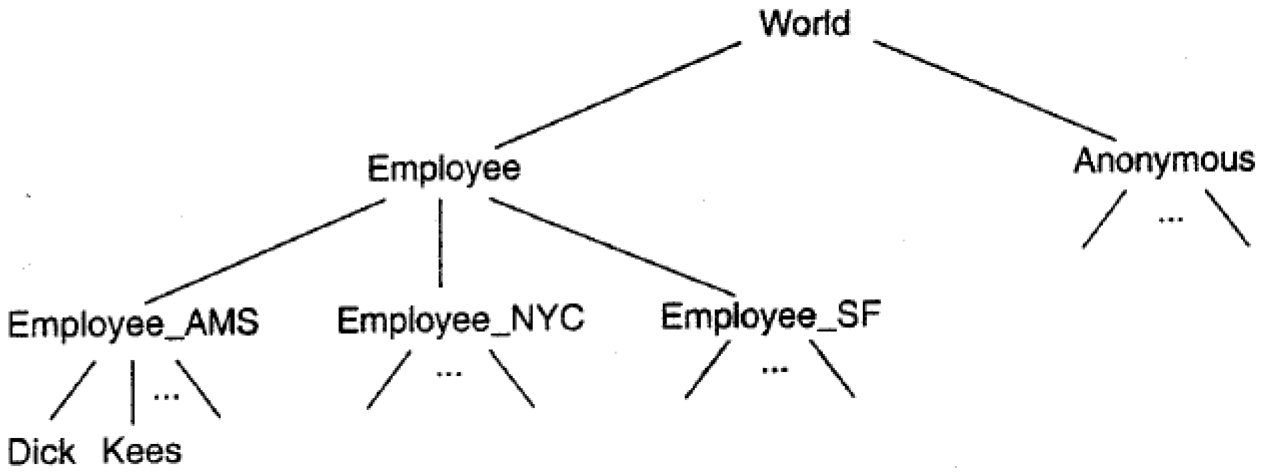

Client
Create access request r for object o. Pass capability C
(o, r) C
Server
Object
if (r appears in C) grant access;

Access Control

ACL or a capability list can become quite large

Access Control

- **Protection Domain**: I
  - Is a set of (object, access rights) pairs. Each pair specifies for a given object exactly which operations are allowed to be carried out
  - Each subject associated with a protection domain group Eg hierarchical organization of groups



Disadvantage: looking up group membership details from database can be time consuming

Access Control

•each subject carry a **certificate listing the groups it belongs to.**

•Whenever Dick wants to read a Web page from the company's intranet, he hands over his certificate to the reference monitor stating that he is a member of *Employee-AMS.*

• *Protect certificate with digital signature -* comparable to capabilities.

Access Control

- **Protection Domains as Roles:**
  - Role-based access control, a user logs into the system with a specific role, which is often associated with a function the user has in an organization
  - User may have several functions. For example, Dick could simultaneously be head of a department, manager of a project, and member of a personnel search committee.
  - Depending on the role he takes when logging in, he may be assigned different privileges.
  - Hence role determines the protection domain (i.e., group) in which he will operate.

Firewalls

Access control based on ACL fine for controlling resources to be accessed by components of a Distributed System

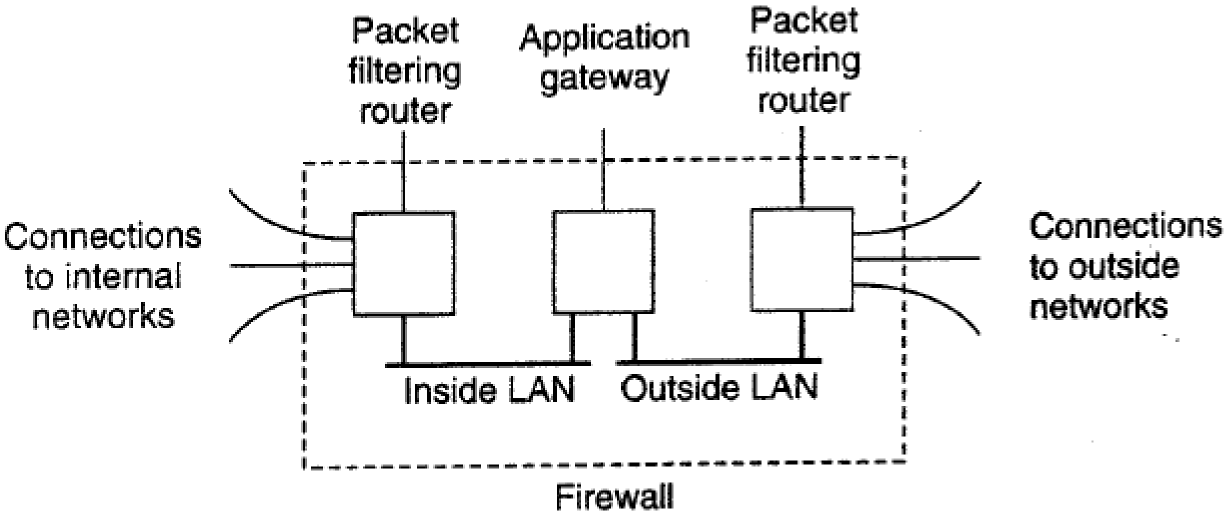
For outside world access of resources accesses including sending mail, downloading files, uploading require firewall -
disconnects any part of a distributed system from the outside world,

All outgoing, but especially all incoming packets are routed through a special computer and inspected before they are passed.

Unauthorized traffic is discarded and not allowed to continue.

An important issue is that the firewall itself should be heavily protected against any kind of security threat: it should never fail.

Firewalls



packet-filtering gateway.
 - This type of firewall operates as a router and makes decisions as to whether or not to pass a network packet based on the source and destination address as contained in the packet's header.
Eg: protect an internal Web server against requests from hosts that are not on the internal network, a packet-filtering gateway could decide to drop all incoming packets addressed to the Web server

Firewalls

application-level gateway.

- this type of firewall actually inspects the content of an incoming or outgoing message.

A typical example is a mail gateway that discards incoming or outgoing mail exceeding a certain size.

proxy gateway.:

- front end to a specific kind of application, and ensures that only those messages are passed that meet certain criteria

- many Web pages contain scripts or applets that are to be executed in a user's browser. To prevent such code to be downloaded to the inside LAN, all Web traffic could be directed through a Web proxy gateway.

Secure Mobile Code

- It is code that can migrate between hosts instead of just migrating passive data
- Threats:
  - Owner will want to protect it against malicious hosts that try steal or modify information carried by the agent.
  - Hosts need to be protected against malicious agents (trusted or corrupt) access control

problem: the program should not be allowed unauthorized access to the host's resources.

Secure Mobile Code

•Example mobile agent searching for cheapest ticket between two places with the intent to make reservations as soon as it finds one.

- Agent moves to a host, host should not be allowed to steal the agent's credit card information
- Agent should be protected against modifications that make the owner pay much more than actually is needed

•Three mechanisms as in Ajanta system for agent's owner to detect that the agent has been tampered with:

i read-only state
ii append only logs
iii selective revealing of state to certain servers

Ajanta system

- Read only state
  - collection of data items to be signed by the agent's owner before sending to host (message digest by encrypting using private key)
  - agent arrives at a host, that host can easily detect whether the read-only state has been tampered with by verifying the state against the signed message digest of the original municipal

- secure append-only logs.
  - collect information while moving between hosts
  - data can be removed or modified without the owner

Ajanta System

- selective revealing of state -
  - providing an array of data items, where each entry is intended for a designated server
  - Each entry is encrypted with the designated server's public key to ensure confidentiality.
  - Entire array is signed by the agent's owner to ensure integrity of the array as a whole

Protecting the Host

- Protecting hosts against malicious mobile code
- Sandboxing
  - A technique by which a downloaded program is executed in such a way that each of its instructions can be fully controlled.
  - If an attempt is made to execute an instruction that has been forbidden by the host, execution of the program will be stopped.
  - Execution is halted when an instruction accesses certain registers or areas in memory that the host has not allowed.

Java Sandboxing

➢Java program is compiled to a set of instructions that are interpreted by what is called the Java Virtual Machine (JVM).

➢JVM handles actual execution of downloaded program by interpreting each of its instructions, starting at the instructions that comprise main.

➢Sandboxing

- ensuring that the component that handles the transfer of a program to the client machine can be trusted
- exclusively trusted class loaders are used
- Java program is not allowed to create its own class loaders
- byte code verifier checks whether a downloaded class obeys the security rules of the sandbox
- verifier checks that the class contains no illegal instructions or
- instructions that could somehow corrupt the stack or memory

Denial of Service

- maliciously preventing authorized processes from accessing resources.

 - huge collection of processes jointly attempt to bring down a networked service

-the attackers have succeeded in hijacking a large group of machines which unknowingly participate in the attack

- Target bandwidth depletion (simply sending many messages to a single machine, so that normal messages will hardly be able to reach the receiver)
- Resource depletion (receiver use up resources on otherwise useless messages,

Eg: TCP SYN-flooding. In this case, the attacker attempts to initiate a huge amount of connections (i.e., send SYN packets as part of the three-way handshake),

but will otherwise never respond to acknowledgments from the receiver.

Denial of Server

➢Remedies:

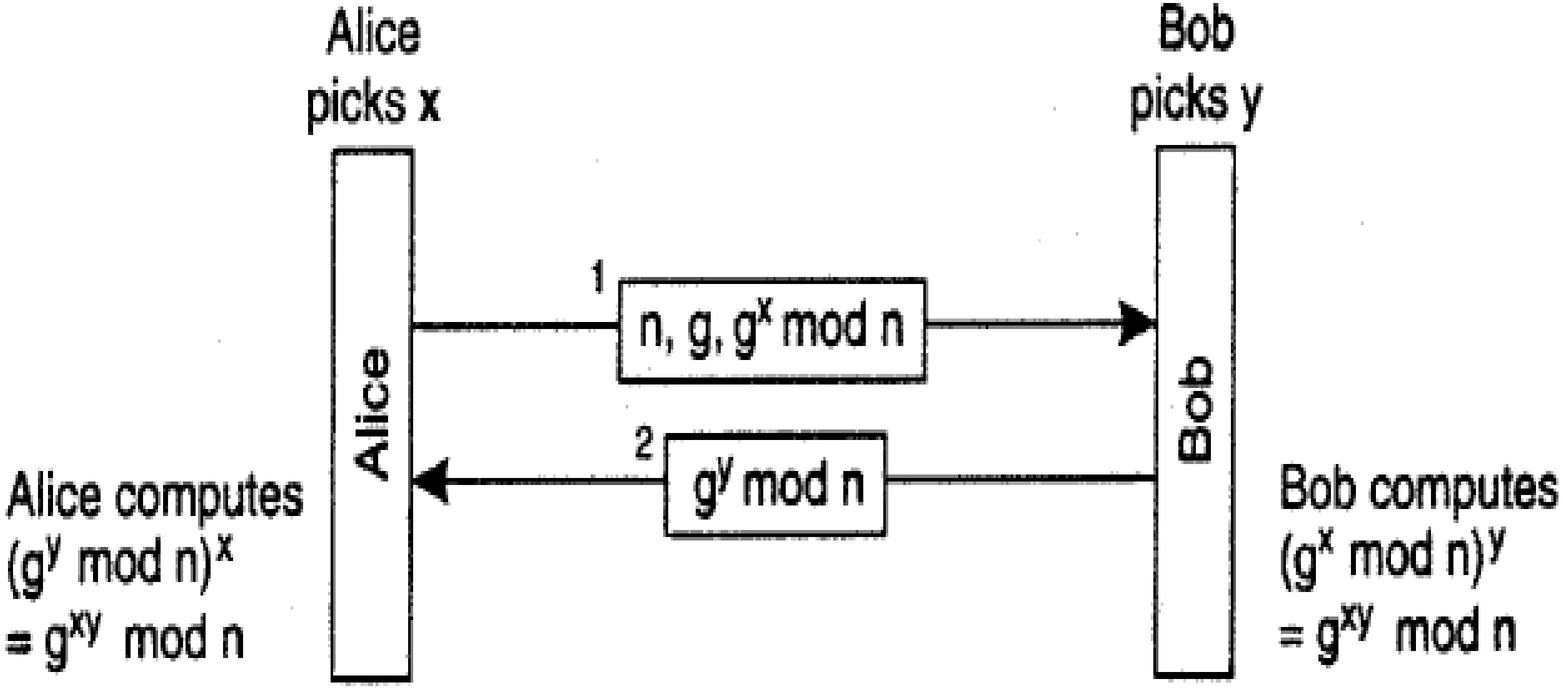
- secretly installing software on their machines – virus detection

- monitor network traffic - dropping packets whose source address does not belong to the organization's network

- Routers at ISP level start dropping packets when they suspect that an attack is going on router will drop packets when it notices that the rate between the number of packets to a specific node is disproportionate to the number of packets from that node.

Key Distribution

Distribute Keys through secure channel
Revocation of key



Key Distribution

public-key distribution takes place by means of public-key certificates. Such a certificate consists of a public
key together with a string identifying the entity to which that key is associated.

Certificate Distribution Authority
Revocation List

THANKS