Security in mobile and wireless computing

INTRODUCTION

Technological transition is marked by the convergence Of the telecommunications infrastructure with that of IP data networking to provide integrated voice, video, and data services.

The technologies related to wireless communication can be complex to differentiate.

Wireless technology has been around for a while; there has been the evolution of new wireless standards to support the voice, video and data communication.

Contd…

- **INTRODUCTION**

There is interest in creating mobile computing labs utilizing laptops computers equipped with wireless ethernet cards.

Industry has made significant progress in resolving some constraints to the widespread adoption of wireless technologies.

Wireless technologies can both support the institution mission and provide cost-effective solutions. Wireless is being adopted for many new applications:

- To connect computers
- To allow remote monitoring and data acquistion
- To provide access control and secrity.
- To provide a solution for environments where wires may not be the best solution.

There are two kind of mobility:

USER MOBILITY: This means that a user can access the same services at different location s, for eg. Call forwarding and roming services provided by telephone.

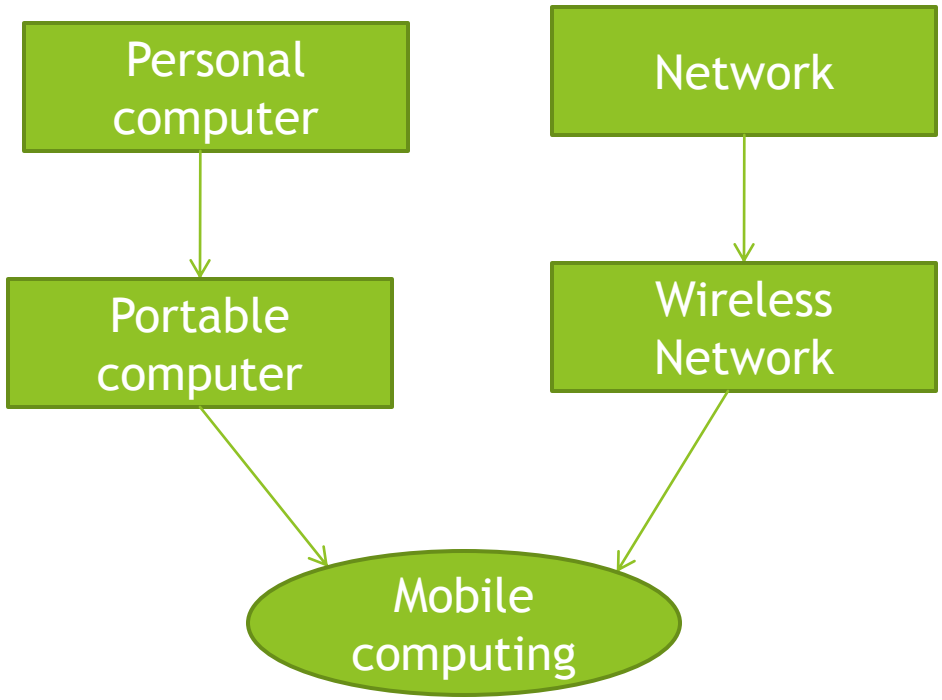
DEVICE MOBILITY: This means that the communication device moves. For eg. Mobile phones. whereas wireless is used only in with regard to devices, without wires.

Characteristics of communication devices:

These devices can exhibit one of the following characteristics:

FIXED AND WIRED
MOBILE AND WIRED
FIXED AND WIRELESS
MOBILE AND WIRELESS

How technologies converged to form mobile computing



Technical challenges of mobile computin

- Disconnection
- Low bandwidth
- High bandwidth variability
- Low power and resources
- Security risks
- Wide variety terminals and devices with different capabilities
- Device attributes
- Fit more functionality into single, smaller device

Mobile Applications

- For Estate Agents
- In courts
- In companies
- Stock Information Collection/Control
- Credit Card Verification
- Taxi/Truck Dispatch
- Electronic Mail/Paging

Mobile and wireless devices

- Laptops
- Palmtops
- PDAs
- Cell phones
- Pagers
- Sensors

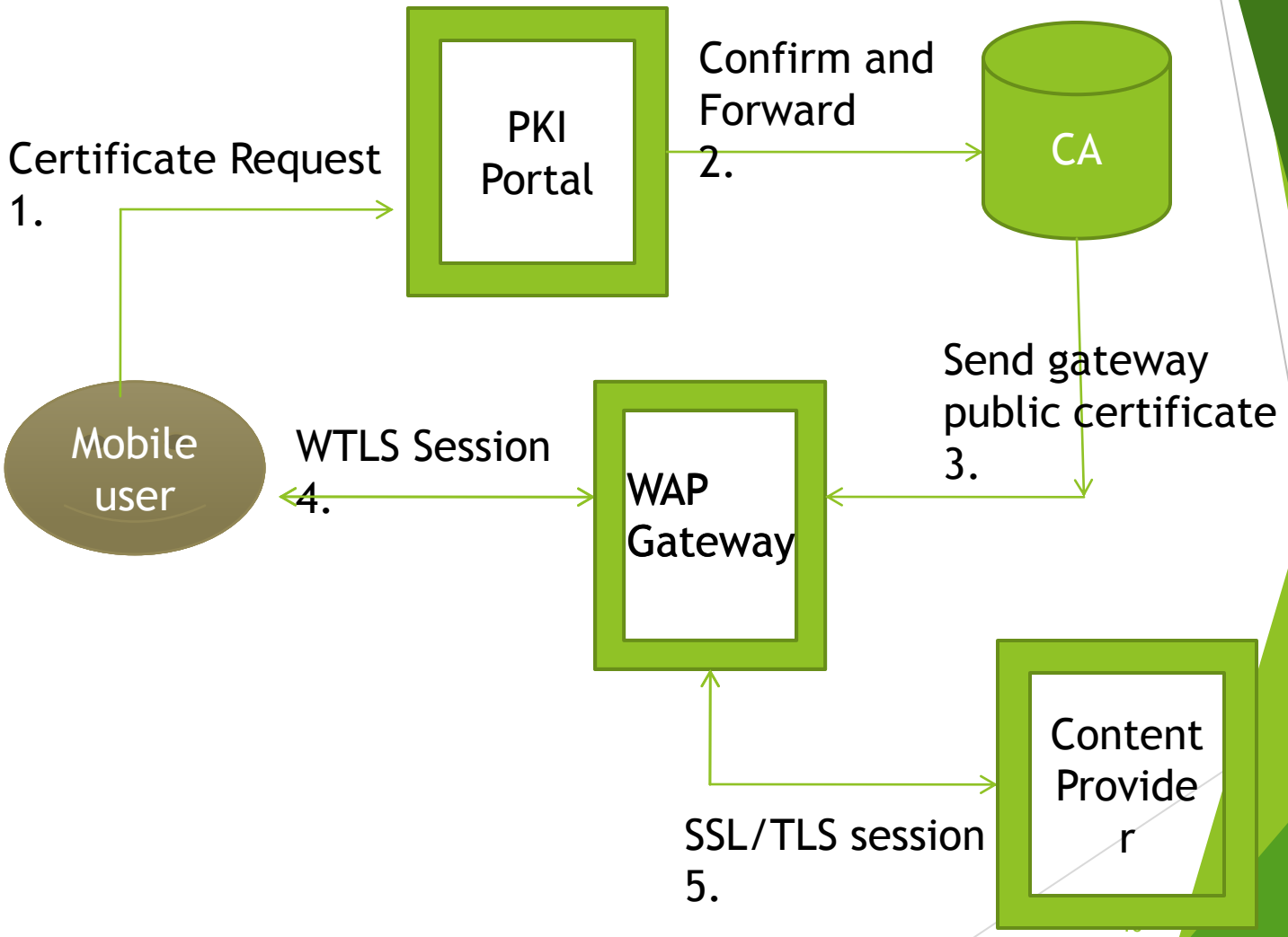
Security levels of mobile communication

Level 1 Security: It is implemented by pass code identification. The user sends a pass code to the mobile network. Then the pass code is compared with the one in the device database.

Level 2 Security: it is implemented by symmetric key schemes as presented in figure. The main feature is that the client is able to authenticate the identity of the gateway. Currently WTLS (Wireless Transport Layer Security) session is established between the WAP client and the gateway. Future version of WAP will alow a WTLS session to terminate beyond the gateway. In this way the routing is via gateway, but communication is not transparent to the gateway.

Cont…

Security levels of mobile communication



Level 2 secure mobile communication

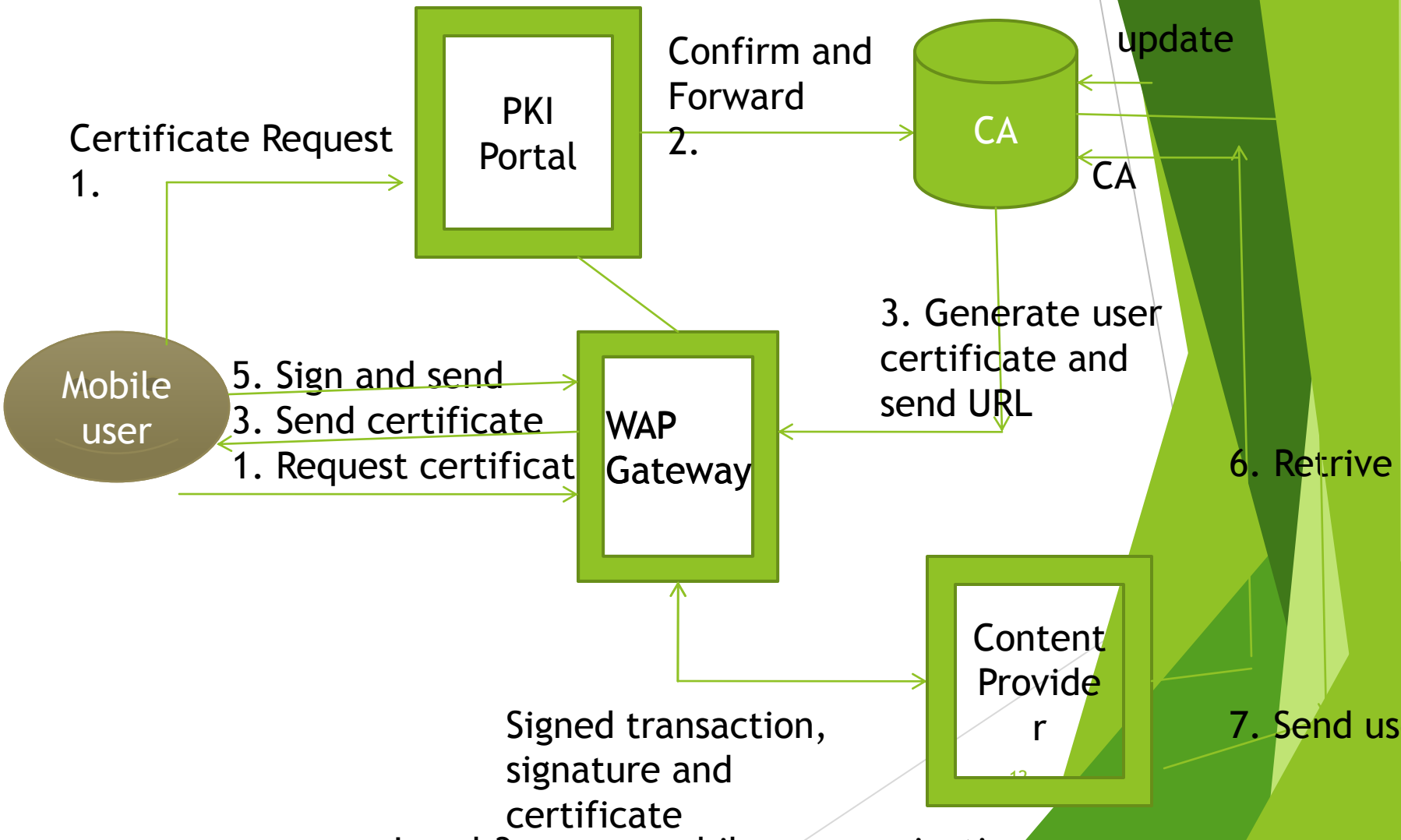
Security levels of mobile communication

The mobile device possesses partial or complete CA root public key information. The WAP gateway generates a key pair: public key and private key. The protocol continues as follows:

1. Gateway sends certificate request to PKI portal.
2. PKI portal confirms the gateway ID and forwards the request to CA.
3. CA sends gateway public certificate to client.
4. WTLS (Wireless Transport Layer Security) session is established between the mobile device and the gateway.
5. SSL connection is established between the gateway and the content provider server.

Level 3 security is implemented by asymmetric key schemes. The client is able to authenticate gateway's identity. Equally, the gateway can ask the user to prove the possession of the private keys with the same ID. The gateway sends some data to the user. The user signs with his private keys and sends back to the server, which verifies the user's signature.

Security levels of mobile communication



Level 3 secure mobile communication

Root CA public keys must be provisioned in both the mobile device and the server. The Crypto.signText function provides a means for a client device to create a digital signature and sends it using WML scripts.

1. The client requests a certificate from PKI portal via gateway.
2. PKI portal confirms the user ID and forwards the request to the CA.
3. CA generates user certificate and sends certificate URL to the client.CA may choose to send the complete client certificate to the device. It can be stored on the SIM card.
4. If necessary, CA updates the database with user public key certificate.
5. The client signs the transaction and sends the transaction, signature and certificate URL to the content provider via gateway. The server may be possess the certificate.
6. The server uses certificate URL to retrieve user certificate from CA database.
7. CA sends the user certificate to the server.

Authentication methods

The fundamental problem is that of authenticating a human to a machine. The human, can be authenticated to a machine based on any combination of the following:

Three factors:

- something you have — *key, card*
  - can be stolen
- something you know — *passwor*
  - can be guessed, shared, stolen
- something you are — *biometrics*
  - costly, can be copied (sometimes)

Authentication

factors may be combined

- ATM machine: 2-factor authentication
  - ATM card *something you have*
  - PIN *something you know*

Reusable passwords

- Keep a database of username:password mappings
- Prompt for a user name & password
- Look up the corresponding password in a database (file) to authenticate

```
if (supplied_password == retrieved_password)
        user is authenticated
```

- This is also known as the Password Authentication Protocol (PAP)

Reusable passwords

One problem: what if the password file isn't sufficiently protected and an intruder gets hold of it, he gets all the passwords!

Enhancement:

Store a hash of the password in a file

- given a file, you don't get the passwords
- have to resort to a dictionary or brute-force attack

Reusable passwords

Passwords can be stolen by observing a user's session over the network:

- snoop on telnet, ftp, rlogin, rsh sessions
- Trojan horse
- social engineering
- brute-force or dictionary attacks

Kerberos

- authentication service developed by MIT
  - project Athena 1983-1988
- trusted third party
- symmetric cryptography
- passwords not sent in clear text
  - assumes only the network can be compromised

Kerberos

Users and services authenticate themselves to each other

To access a service:

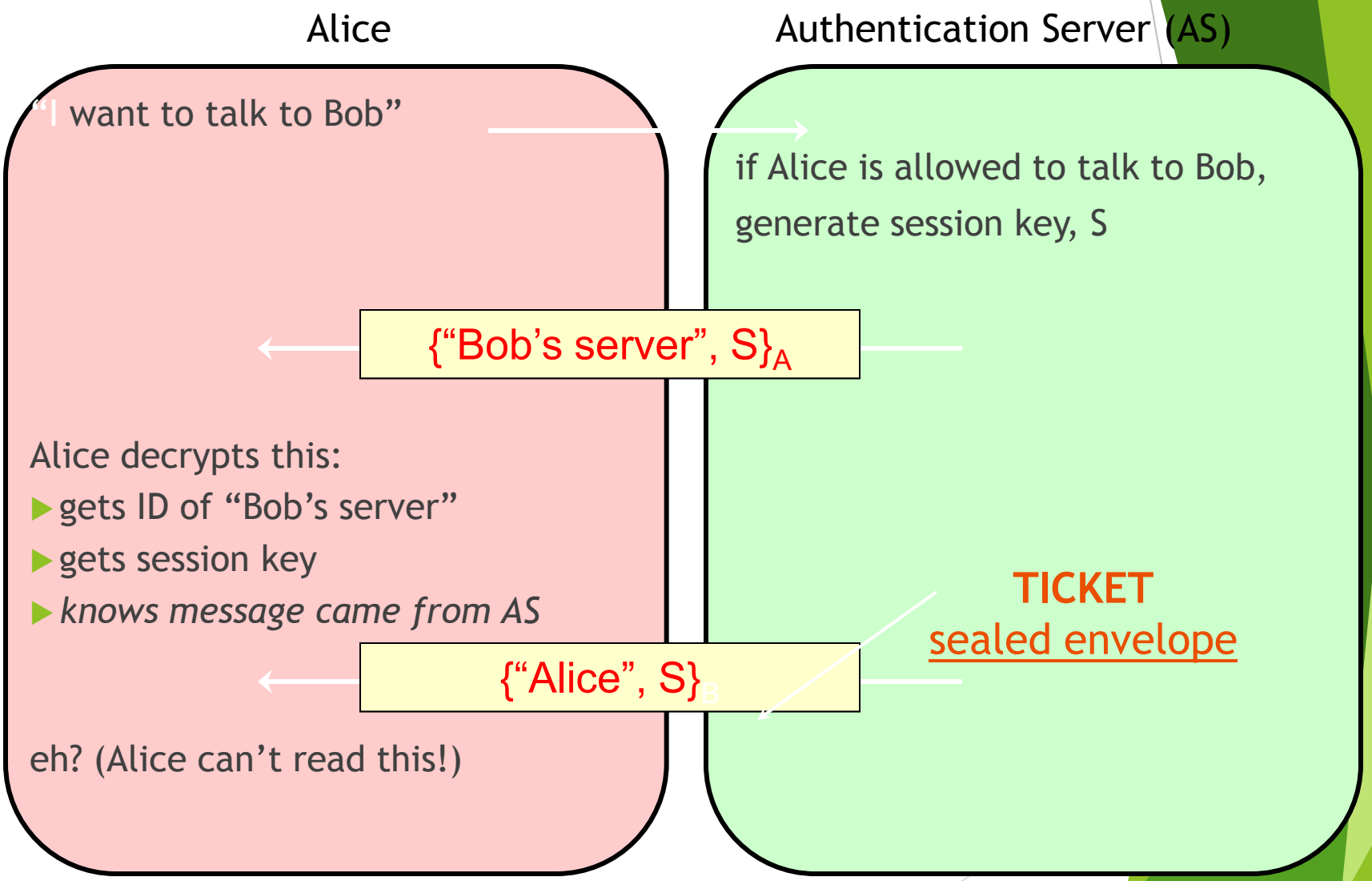
- user presents a ticket issued by the Kerberos authentication server
- service examines the ticket to verify the identity of the user

Kerberos

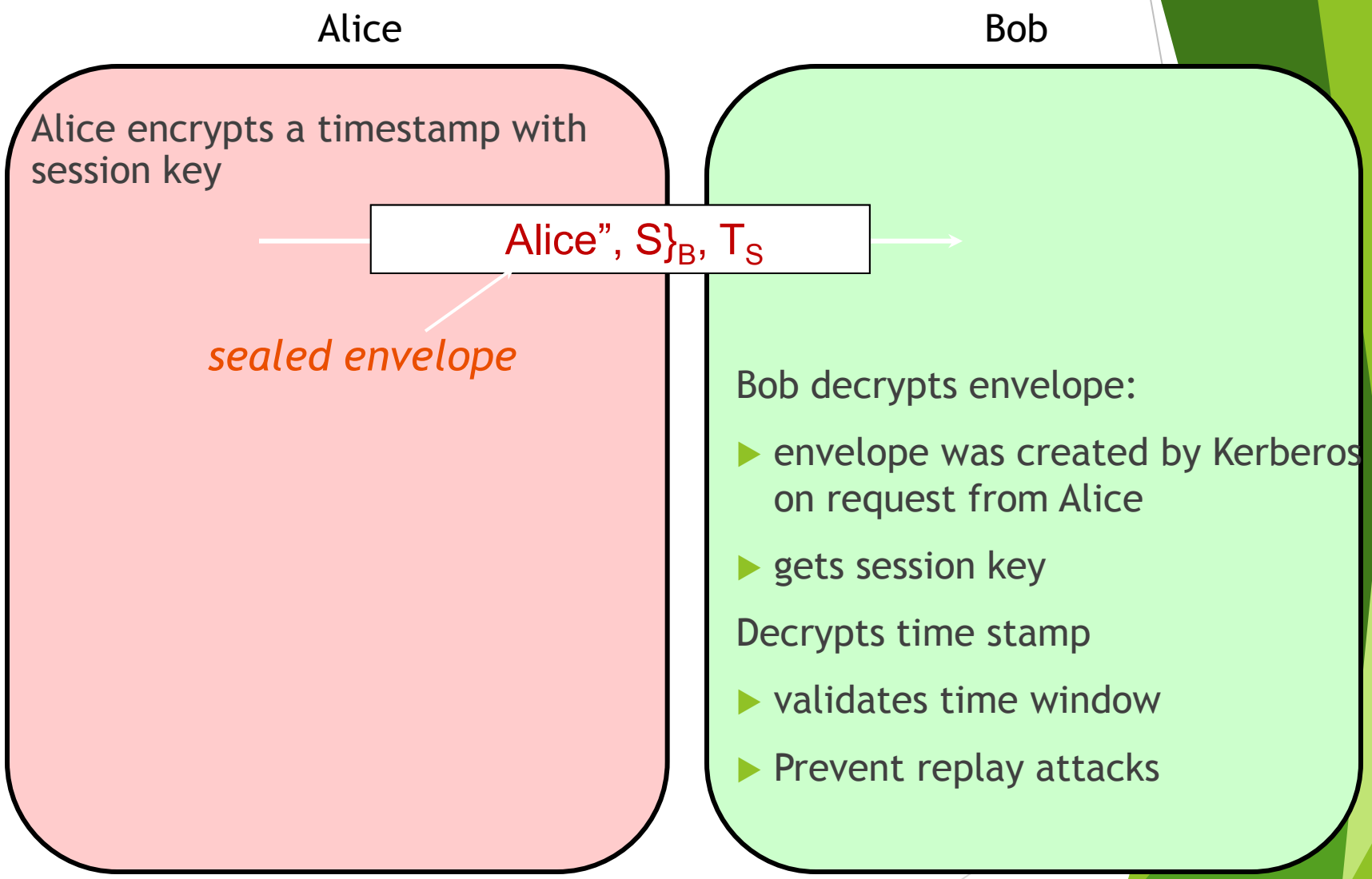
- user *Alice* wants to communicate with a service *Bob*
- both Alice and Bob have keys

- Step 1:
  - Alice authenticates with Kerberos server
    - Gets session key and ***sealed envelope***
- Step 2:
  - Alice gives Bob a session key (securely)
  - Convinces Bob that she also got the session key from Kerberos

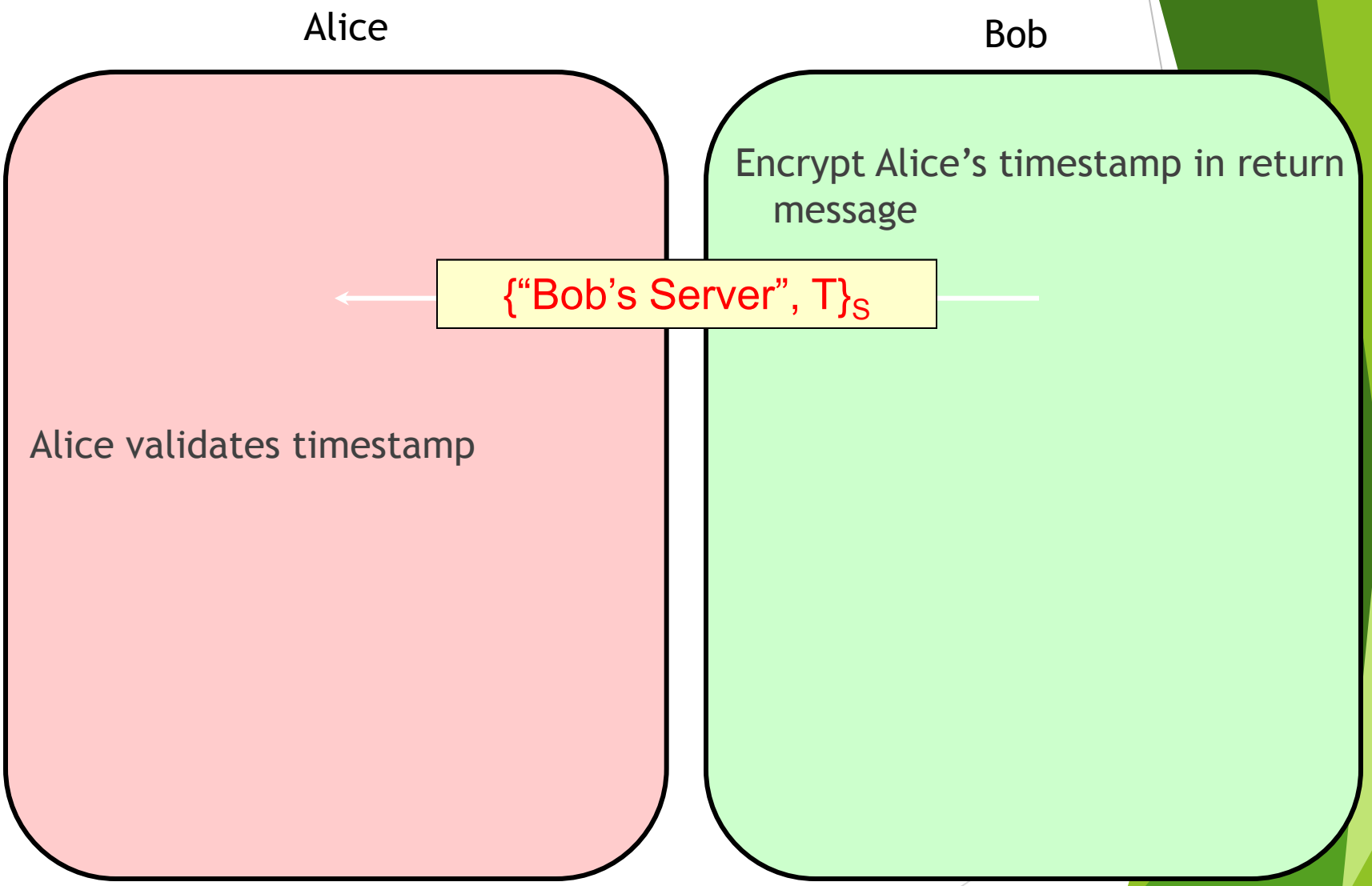
Authenticate, get permission



Send key


Alice
Bob
Alice encrypts a timestamp with session key
Alice", S}B, TS
sealed envelope
Bob decrypts envelope:
envelope was created by Kerberos on request from Alice
gets session key
Decrypts time stamp
validates time window
Prevent replay attacks

Authenticate recipient



Kerberos key usage

- Every time a user wants to access a service
  - User's password (key) must be used each time (in decoding message from Kerberos)
- Possible solution:
  - Cache the password (key)
  - Not a good idea
- Another solution:
  - Split Kerberos server into Authentication Server + Ticket Granting Server

Authentication Protocols

Authentication protocols overview

Authentication is a fundamental aspect of system security. It confirms the identity of any user trying to log on to a domain or access network resources. Windows Server 2003 family authentication enables single sign-on to all network resources. With single sign-on, a user can log on to the domain once, using a single password or smart card, and authenticate to any computer in the domain.

Authentication types

When attempting to authenticate a user, several industry-standard types of authentication may be used, depending on a variety of factors. The following table lists the types of authentication that the Windows Server 2003 family supports.

Types of authentication protocol

Authentication protocols	Description
Kerberos V5 authentication	A protocol that is used with either a password or a smart card for interactive logon. It is also the default method of network authentication for services.
SSL/TLS authentication	A protocol that is used when a user attempts to access a secure Web server.
NTLM authentication	A protocol that is used when either the client or server uses a previous version of Windows.
Digest authentication	Digest authentication transmits credentials across the network as an MD5 hash or message digest.
Passport authentication	Passport authentication is a user-authentication service which offers single sign-in service.

Laptops Security

Laptops have become thief magnets, attracting everything from dishonest housekeeping employees to sophisticated conmen, hi-tech crime rings, and industrial spies. In 1999 alone, over 319,000 laptops were reported stolen. Thousands more were simply misplaced or left in hotel rooms, restaurants, airports, cabs or coffee shops by busy employees rushing around. Protect your capital investment and your company's secrets by following these guidelines to better laptop security.

Basic Security Measures:

Choose a secure operating system and lock it down
If you care about your data, pick an operating system that is secure. Windows 2000 Professional and Windows XP Professional both offer secure logon, file level security, and the ability to encrypt data. If you are running Windows 95/98/Me, anyone who picks up your laptop can access your data.

Enable a strong BIOS password
Foil would be data thieves right from the start by password protecting the BIOS. Some laptop manufacturers have stronger BIOS protection schemes than others, so do some homework before relying on this alone. Find out from your laptop manufacturer what the procedure is for resetting the BIOS password. If they absolutely demand that you send it back into the factory and don't give you a "workaround", you'll have a better chance of recovering the machine and maybe even catching the thief. (Both IBM and Dell scored well in our field tests) Also find out if the BIOS password locks the hard drive so it can't simply be removed and reinstalled into a similar machine.

Asset Tag or Engrave the laptop

Permanently marking (or engraving) the outer case of the laptop with your company name, address, and phone number may greatly increase your odds of getting it returned to you if you happen to carelessly leave it in a hotel room. There are also a number of metal tamper resistant commercial asset tags available that could help the police return your hardware if it is recovered. According to the FBI, 97% of unmarked computers are never recovered. Clearly marking your laptops deters casual thieves and may prevent it from simply being resold over the internet via an online auction.

Register the laptop with the manufacturer

We've become so used to throwing away the registration cards for all of the electronic items we buy every day, because we've learned that it just leads to more junk mail. Registering your laptop with the manufacturer will "flag" it if a thief ever sends it in for maintenance, and increases your odds of getting it back. It also pays to write down your laptop's serial number and store it in a safe place. In the event your laptop is stolen, it will be impossible for the police to ever recover it if they can't trace it back to you.

Physical security

Get a cable lock and use it

Over 80% of the laptops on the market are equipped with a Universal Security Slot (USS) that allows them to be attached to a cable lock or laptop alarm. While this may not stop determined hotel thieves with bolt cutters, it will effectively deter casual thieves who may take advantage of you while your sleeping in an airport lobby, leaving a table to go the bathroom, etc. And remember: They only work if you use them properly. Tether them to a strong immovable and unbreakable object.

Use a docking station

Unbelievably, almost 40% of laptop theft occur *in the office*. Poorly screened housekeeping staff, contractors, and disgruntled employees are the usual suspects. You can help prevent this by using a docking station that is permanently affixed to your desktop *and* has a feature which locks the laptop securely in place. If you are leaving it overnight, or for the weekend, lock your laptop in a secure filing cabinet in your office and lock your office door.

Lock up your PCMCIA cards

While locking your PC to desk with a cable lock may keep someone from walking away with your laptop, there is little you can do to keep someone from stealing the PCMCIA NIC card or modem that is sticking out of the side of your machine. When not in use, eject these cards from the laptop bay and lock them in a safe place. Your docking station should have a NIC card built into it at your desk, and if you are traveling you won't be connected to the network anyway. Even when they aren't being used, PCMCIA cards still consume battery power and contribute to the heat levels within your laptop

Use a personal firewall on your laptop

Corporate networks protect their Servers and Workstations by configuring a firewall to prevent intruders from hacking back into their systems via the company's internet connection. But once users leave the corporate buildings and connect to the web from home or a hotel room, their data is vulnerable to attack. Personal firewalls such as BlackIce and ZoneAlarm are an effective and inexpensive layer of security that take only a few minutes to install. Although Windows XP comes with a personal firewall, it does not attempt to manage or restrict outbound connections at all. We recommend using a good third-party personal firewall to secure your Windows XP workstations. If you want to test how much information your personal firewall "leaks out" to the web

Use tracking software to have your laptop call home

There are a number of vendors that offer stealthy software solutions that enable your laptop to check in to a tracking center periodically using a traceable signal. In the event your laptop is lost or stolen, these agencies work with the police, phone company, and internet service providers to track and recover your laptop. CompuTrace, SecureIT, Stealth Signal, and ZTrace provide tracking services for corporations and individuals.

Protecting sensitive data

Use the NTFS file system

Assuming your using Windows NT/2000/XP on your laptop, use the NTFS file system to protect your data from laptop thieves who may try to access your data. FAT and FAT32 File systems don't support file level security and give hackers a big wide open door to your system.

Disable the Guest Account

Windows 2000 finally disables the guest account by default, but if you didn't build the image yourself, always double check to make sure the guest account is not enabled. For additional security assign a complex password to the account anyway, and restrict its logon 24x7.

Rename the Administrator Account

Many hackers will argue that this won't stop them, because they will use the SID to find the name of the account and hack that. Our view is, why make it easy for them. Renaming the Administrator account will stop some amateur hackers cold, and will annoy the more determined one. If you rename the account, try not to use the word 'Admin" in its name. Pick something that won't sound like it has rights to anything.

Enable EFS (Encrypting File System)

Windows 2000 ships with a powerful encryption system that adds an extra layer of security for drives, folders, or files. This will help prevent a hacker from accessing your files by physically mounting the hard drive on another PC and taking ownership of files. Be sure to enable encryption on Folders, not just files. All files that are placed in that folder will be encrypted

Disable the Infrared Port on you laptop

I don't know anybody who actual transmits data via the infrared port on their laptop, but we have been able to use the IR port to browse someone else's files from across a conference room table without them knowing it. Disable the IR port via the BIOS, or simply cover it up with a small piece of black electrical tape.

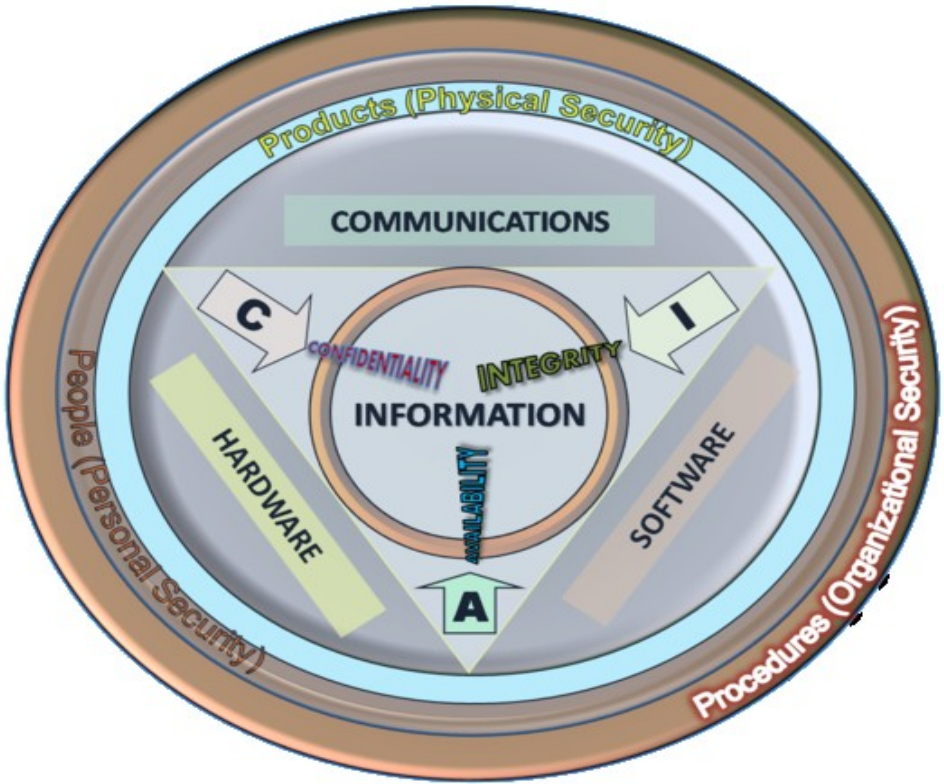
Backup your data before you leave

Many companies have learned the hard way that the data on your computer is more expensive to replace than the hardware. Always backup you laptop before you do any extended traveling that may put your data at risk. This doesn't have to to take a lot of time, and you can use the built in backup utilities that come with Windows 2000. If your network doesn't have the disk space to backup all of your traveling laptop users, you may wish to look into some of personal backup solutions including external hard drives, CD-R's, and tape backup.

Information security

Information security means protecting information **and** information systems **from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.**

The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them.



These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration.
Information security is **concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.**
Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer.
Governments, military, corporations, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers.

Should confidential information about a business' customers or finances or new product line fall into the hands of a competitor, such a breach of security could lead to lost business, law suits or even bankruptcy of the business. Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement.

For the individual, information security has a significant effect on privacy, which is viewed very differently in different cultures. **The field of information security has grown and evolved significantly in recent years. There are many ways of gaining entry into the field as a career. It offers many areas for specialization including: securing network(s) and allied** infrastructure, securing applications **and** databases, security testing, **information systems** auditing, business continuity planning **and** digital forensics **science, etc.**

Purpose of information security management

Managing computer and network security programs has become an increasingly difficult and challenging job. These changes are continuing to accelerate, making the security manager's job increasingly difficult.

The information security manager must establish and maintain a security program that ensures three requirements:

1. The confidentiality,
2. Integrity, and
3. Availability of the company's information resources

Some security experts argue that two other requirements may be added to these three:

1. Utility and
2. Authenticity (i.e., accuracy).

CONFIDENTIALITY

Confidentiality is the protection of information in the system so that unauthorized persons cannot access it. Many believe this type of protection is of most importance to military and government organizations that need to keep plans and capabilities secret from potential enemies. However, it can also be significant to businesses that need to protect proprietary trade secrets from competitors or prevent unauthorized persons from accessing the company's sensitive information (e.g., legal, personnel, or medical information).

Confidentiality must be well defined, and procedures for maintaining confidentiality must be carefully implemented, especially for standalone computers. A crucial aspect of confidentiality is user identification and authentication

Threats to confidentiality

Confidentiality can be compromised in several ways. The following are some of the most commonly encountered threats to information confidentiality:

- Hackers.
- Masqueraders.
- Unauthorized user activity.
- Unprotected downloaded files.
- Local area networks (LANs).
- Trojan horses.

Hackers

A hacker is someone who bypasses the system's access controls by taking advantage of security weaknesses that the systems developers have left in the system. The activities of hackers represent serious threats to the confidentiality of information in computer systems. Many hackers have created copies of inadequately protected files and placed them in areas of the system where they can be accessed by unauthorized persons.

Masqueraders

A masquerader is an authorized user of the system who has obtained the password of another user and thus gains access to files available to the other user. Masqueraders are often able to read and copy confidential files. Masquerading is a common occurrence in companies that allow users to share passwords.

Unauthorized User Activity

This type of activity occurs when authorized system users gain access to files that they are not authorized to access.

Unprotected Downloaded Files

Downloading can compromise confidential information if, in the process, files are moved from the secure environment of a host computer to an unprotected microcomputer for local processing.

Local Area Networks

LANs present a special confidentiality threat because data flowing through a LAN can be viewed at any node of the network, whether or not the data is addressed to that node.

Trojan Horses

Trojan horses can be programmed to copy confidential files to unprotected areas of the system when they are unknowingly executed by users who have authorized access to those files. Once executed, the Trojan horse becomes resident on the user's system and can routinely copy confidential files to unprotected resources.

Confidentiality Models

Confidentiality models are used to describe what actions must be taken to ensure the confidentiality of information. These models can specify how security tools are used to achieve the desired level of confidentiality.

The most commonly used model for describing the enforcement of confidentiality is the **Bell-LaPadula model.**

- It defines the relationships between objects (i.e., the files, records, programs, and equipment that contain or receive information) and subjects (i.e., the persons, processes, or devices that cause information to flow between the objects).
- The relationships are described in terms of the subject's assigned level of access or privilege and the object's level of sensitivity. In military terms, these would be described as the security clearance of the subject and security classification of the object.
- Subjects access objects to read, write, or read and write information.

❖The Bell-LaPadula model enforces the lattice principle, which specifies that subjects are allowed write access to objects at the same or higher level as the subject, read access to objects at the same or lower level, and read/write access to only those objects at the same level as the subject.

❖ This prevents the ability to write higher-classified information into a lower-classified file or to disclose higher-classified information to a lower-classified individual.

❖Because an object's level indicates the security level of data it contains, all the data within a single object must be at the same level.

❖This type of model is called flow model, because it ensures that information at a given security level flows only to an equal or higher level.

Implementing Confidentiality Models

The trusted system criteria provide the best guidelines for implementing confidentiality models. These criteria were developed by the National Computer Security Center and are published in the *Department of Defense Trusted Computer System Evaluation Criteria* (commonly referred to as the Orange Book), which discusses information confidentiality in considerable detail.

INTEGRITY

Integrity is the protection of system data from intentional or accidental unauthorized changes. The challenge of the security program is to ensure that data is maintained in the state that users expect. Although the security program cannot improve the accuracy of data that is put into the system by users, it can help ensure that any changes are intended and correctly applied.

Examples of government systems in which integrity is crucial include air traffic control systems, military fire control systems (which control the firing of automated weapons), and Social Security and welfare systems. Examples of commercial systems that require a high level of integrity include medical prescription systems, credit reporting systems, production control systems, and payroll systems.

Protecting Against Threats to Integrity

Three basic principles are used to establish integrity controls:

1. granting access on a need-to-know basis,
2. separation of duties,
3. rotation of duties.

Granting access on a need-to-know basis:

Users should be granted access only to those files and programs that they need in order to perform their assigned job functions. User access to production data or source code should be further restricted through use of well-formed transactions, which ensure that users can change data only in controlled ways that maintain the integrity of data.

Separation of duties: To ensure that no single employee has control of a transaction from beginning to end, two or more people should be responsible for performing it — for example, anyone allowed to create or certify a well-formed transaction should not be allowed to execute it.

Rotation of duties: Job assignments should be changed periodically so that it is more difficult for users to collaborate to exercise complete control of a transaction and subvert it for fraudulent purposes.

AVAILABILITY

Availability is the assurance that a computer system is accessible by authorized users whenever needed. Two facets of availability are typically discussed:

1. Denial of service.
2. Loss of data processing capabilities as a result of natural disasters (e.g., fires, floods, storms, or earthquakes) or human actions (e.g., bombs or strikes).

Denial of service usually refers to actions that tie up computing services in a way that renders the system unusable by authorized users. For example, the Internet worm overloaded about 10% of the computer systems on the network, causing them to be nonresponsive to the needs of users.

The loss of data processing capabilities as a result of natural disasters or human actions is perhaps more common. Such losses are countered by contingency planning, which helps minimize the time that a data processing capability remains unavailable.

END OF FIRST UNIT

ASSIGNMENT
UNIT-1

All questions are compulsory and should be hand written.

1. What is data and information. Differentiate between data and information.
2. What is information system? Write types of information system. Explain the need of information Technology in business.
3. What is distributed information system? Explain.
4. What are threat and attacks? Write down the classification of security threats.
5. How to prevent the computer fr0m viruses.
6. Write down the security challenges in mobile devices.. Explain.
7. Explain the security implementation for organization .
8. What is laptop security? How can preventing laptop to theft.
9. What is the purpose of information security management?
10. What is authentication protocol? Write and explain authentication method. Explain with the help of example of any authentication protocol.

Distributed Information Systems

Motivation:

- To understand the problems that Web services try to solve it is helpful to understand how distributed information systems evolved.
- While technology has changed, problems stayed the same.

distributed Information Systems (IS)

- design and related aspects
- architectures
- communication patterns
- scaling

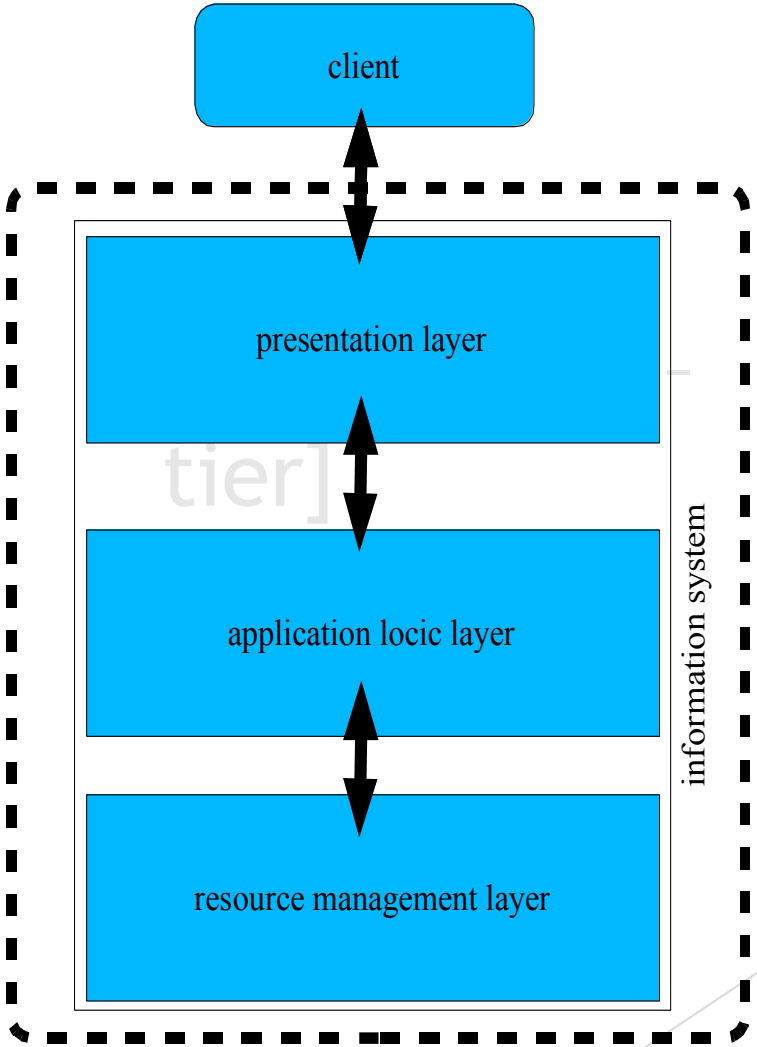
Architecture of an Information System - 4 types:

- *1 - tier*
- *2 - tier*
- *3 - tier*
- *n - tier*

1 – tier Architectures

- were used decades ago..
- monolithic Information Systems
- presentation, application logic, and resource management were merged into a single tier
- many of these 'old' Systems are still in use!

Design of 1 – tier Architecture



1 – tier Architecture

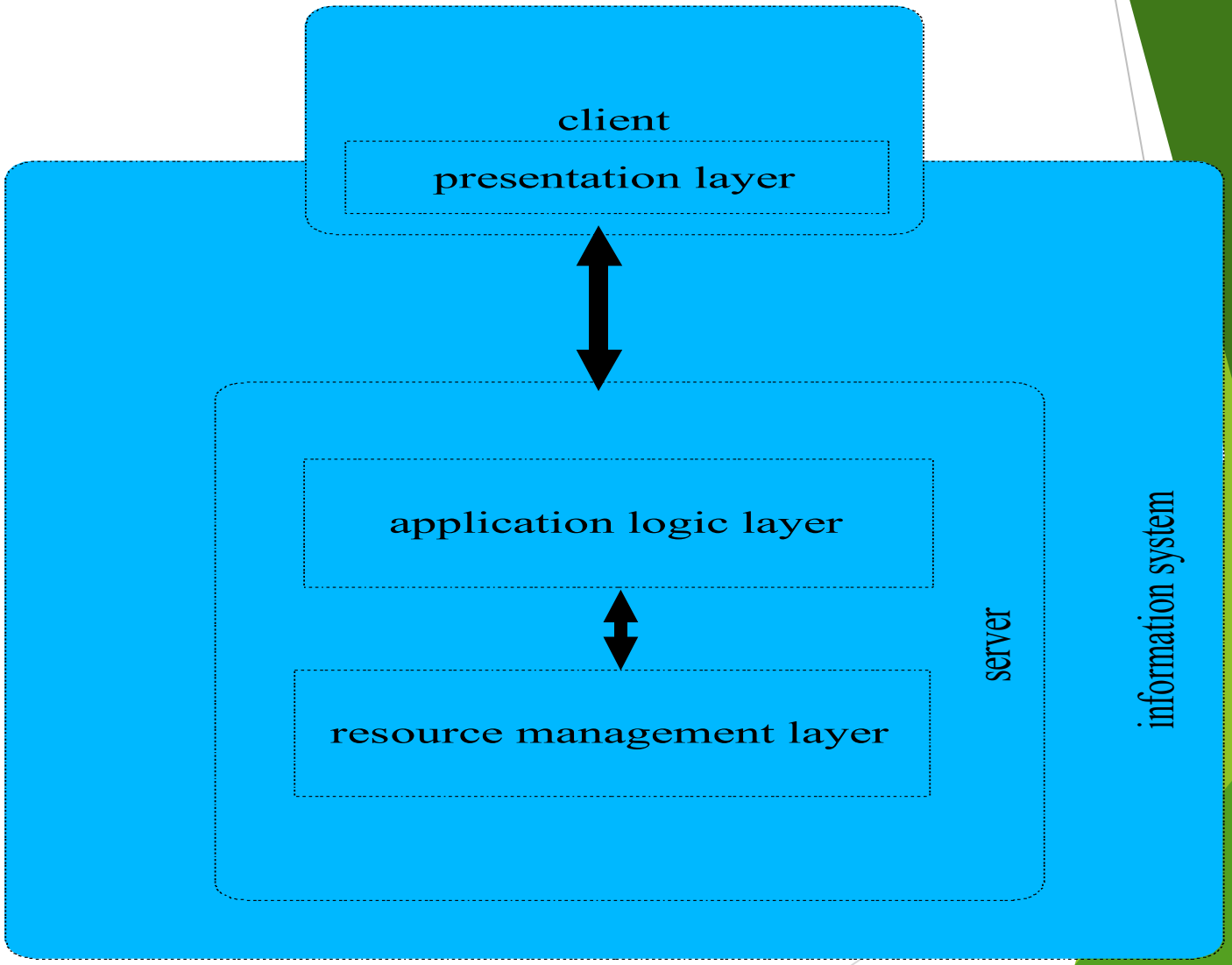
advantages:

- easy to optimize performance
- no context switching
- no compatibility issues
- no client developement, maintainance and deployment cost

disadvantages:

- monolithic pieces of code (high maintainance)
- hard to modify
- lack of qualified programmers for these systems

2 - tier Architectures



2 - tier Architectures

- separation of presentation layer from other 2 layers (app + resource)
- became popular as 'server/client' systems
- thin clients/fat clients
- RPC (Remote Procedure Call)
- API (Application Program Interface)
- need for standardization

advantages & disadvantages

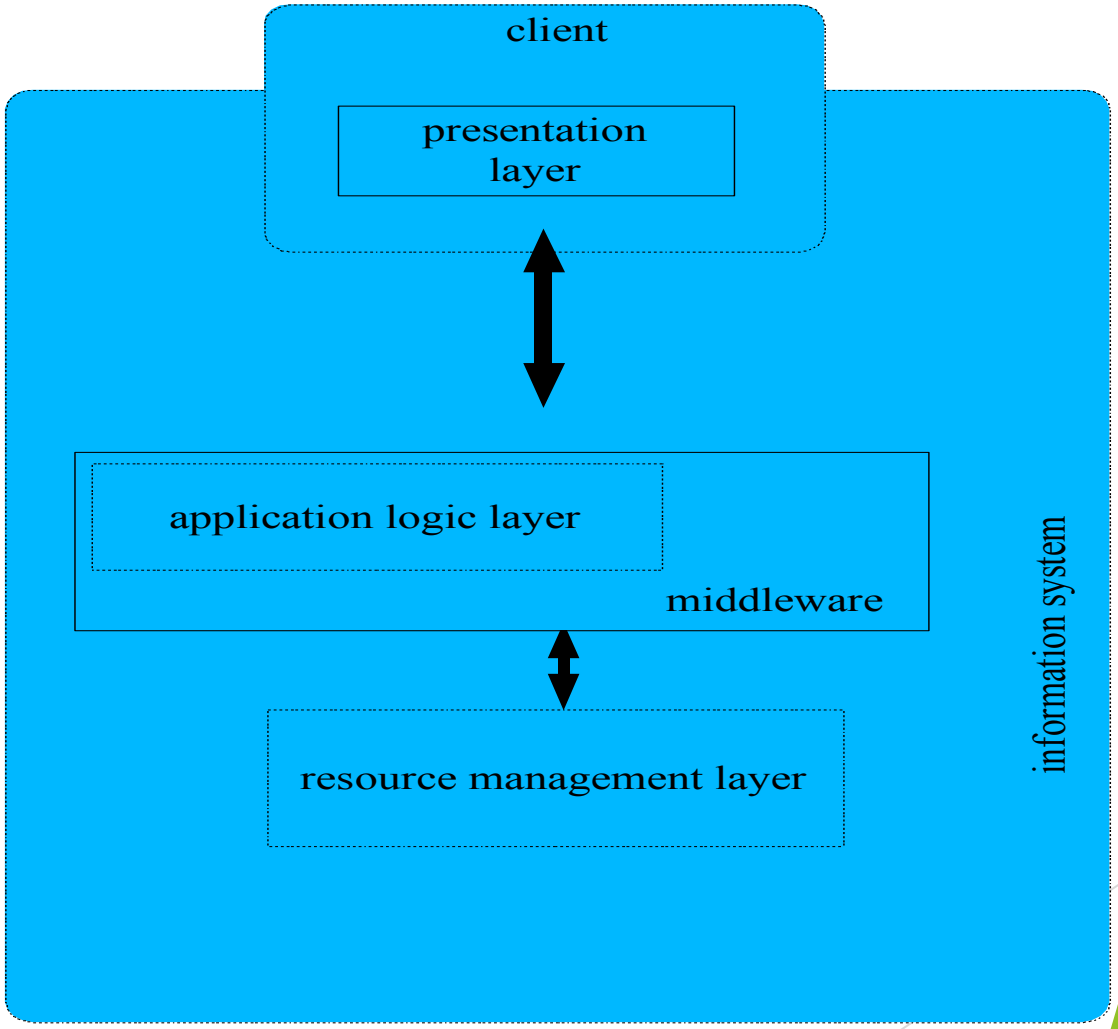
advantages

- portability
- no need for context switches or calls between component for key operations

disadvantages

- limited scalability
- legacy problems (blown up clients)

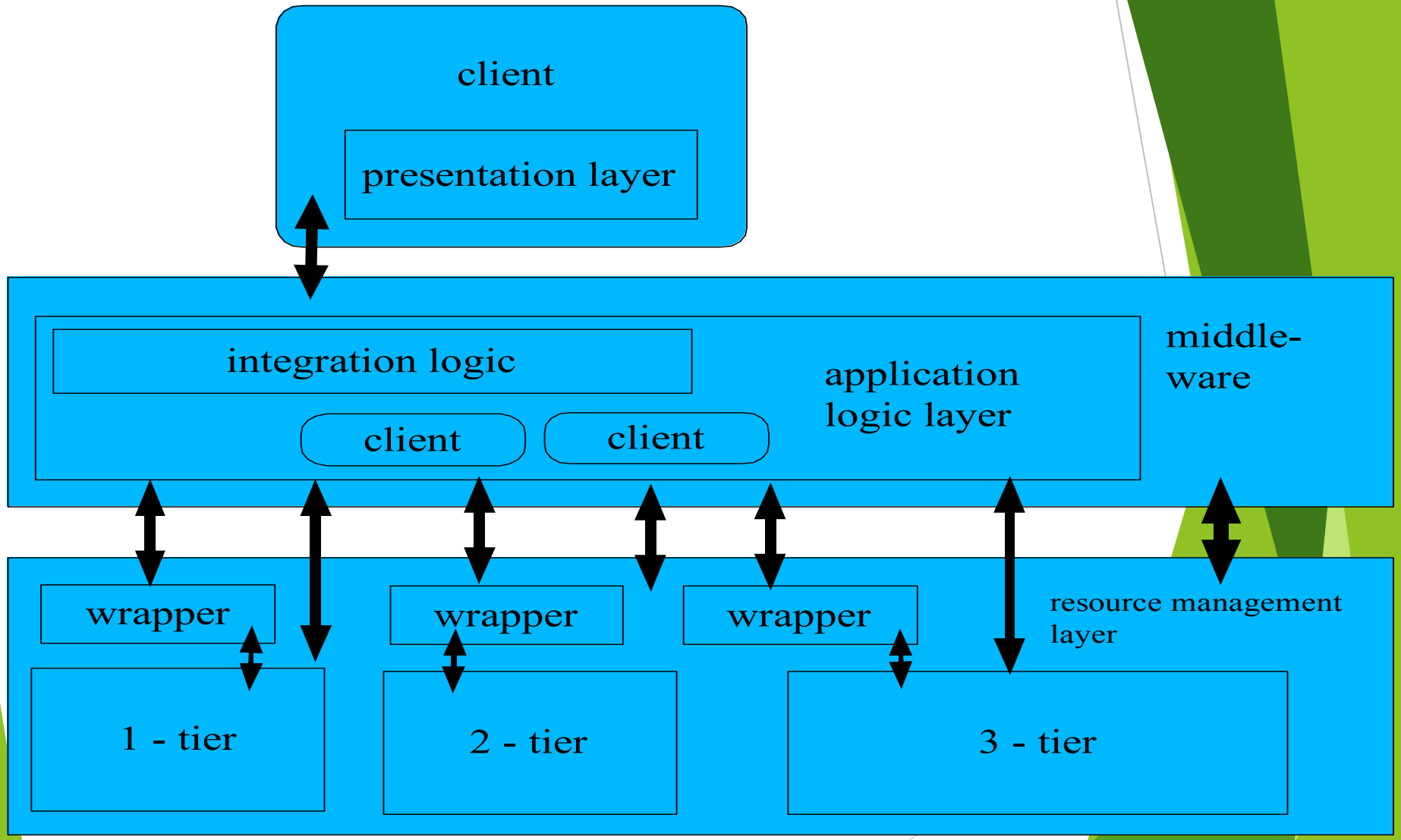
3 - tier Architectures



3 - tier Architectures

- can be achieved by separating RM (resource management) from application logic layer
- additional middleware layer between client and server
  - integration logic
  - application logic
- lead to the introduction of clear RM layer interfaces
- good at dealing with intgration of different resources

3 - tier


client
presentation layer
integration logic
client
client
application logic layer
middle-ware
wrapper
wrapper
wrapper
resource management layer
1 - tier
2 - tier
3 - tier

advantages & disadvantages

advantages

- scalability by running each layer on a different server
- scalability by distributing AL (application logic layer) across many nodes
- additional tier for integration logic
- flexibility

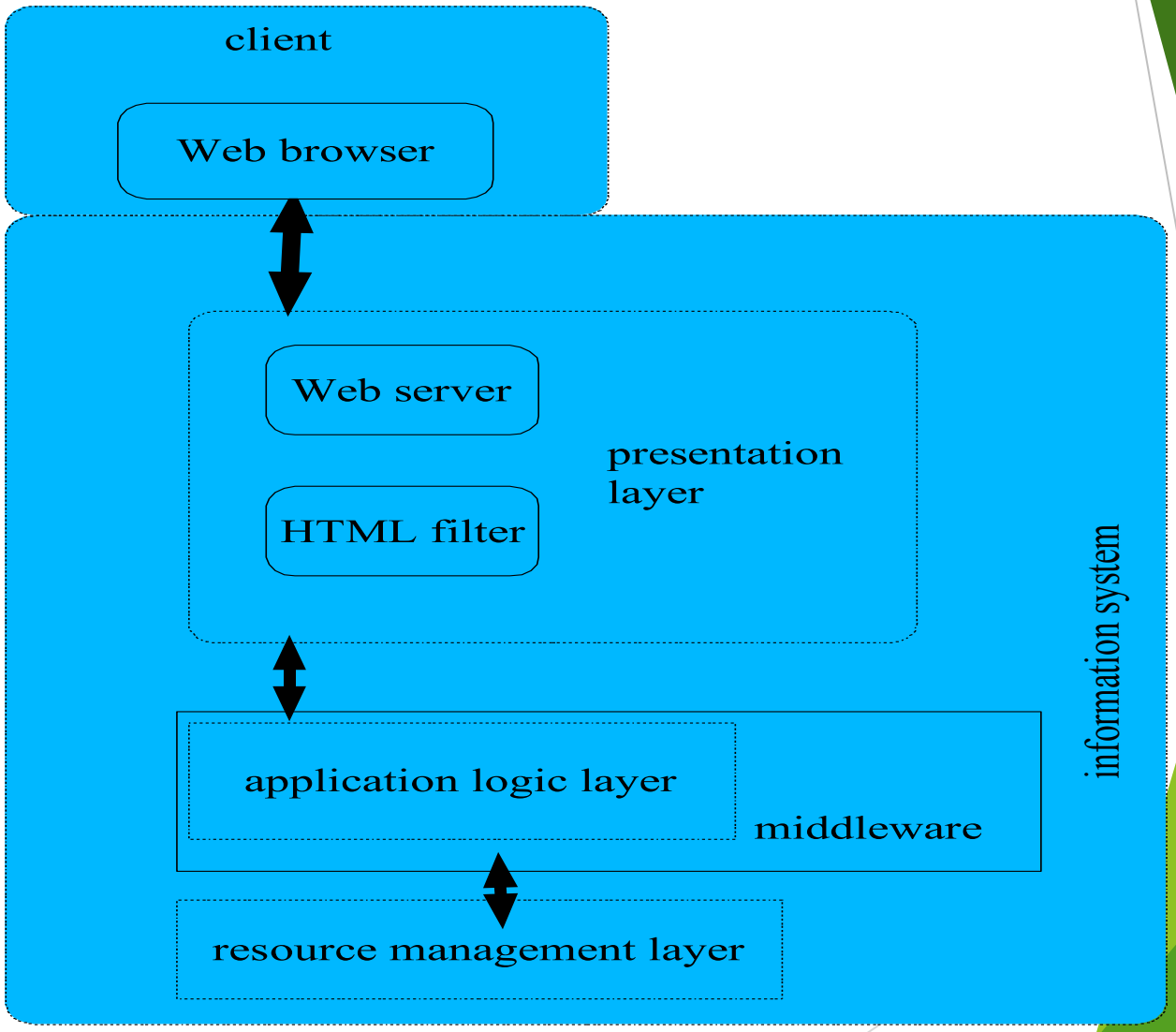
disadvantages

- performance loss if distributed over the internet
- problem when integrating different 3 – tier systems

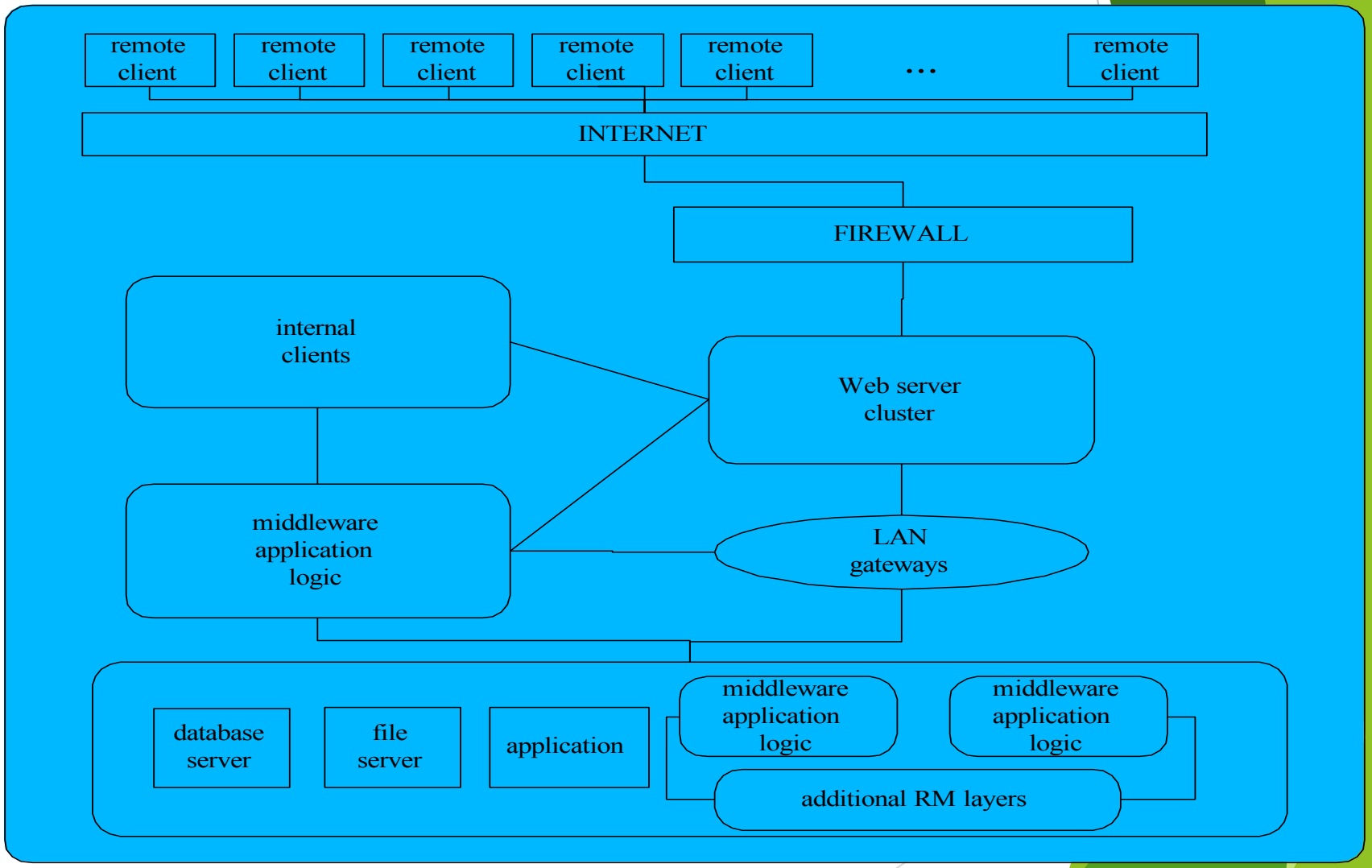
n -tier

- 2 cases of n – tier
- systems linked with added connectivity through the internet
- resource layer is a full fledged 2 - or 3 - tier system

n -tier


client
Web browser
Web server
HTML filter
presentation layer
application logic layer
middleware
resource management layer
information system

n - tier


remote client
remote client
remote client
remote client
remote client
...
remote client
INTERNET
FIREWALL
internal clients
Web server cluster
middleware application logic
LAN gateways
database server
file server
application
middleware application logic
middleware application logic
additional RM layers

advantages & disadvantages

advantages

- better scalability
- higher fault tolerance
- higher throughput for less cost

disadvantages

- too much middleware involved
- redundant functionality
- difficulty and cost of developement

gains and losses

with growing number of tiers one gains:

- flexibility
- functionality
- possibilities for distribution

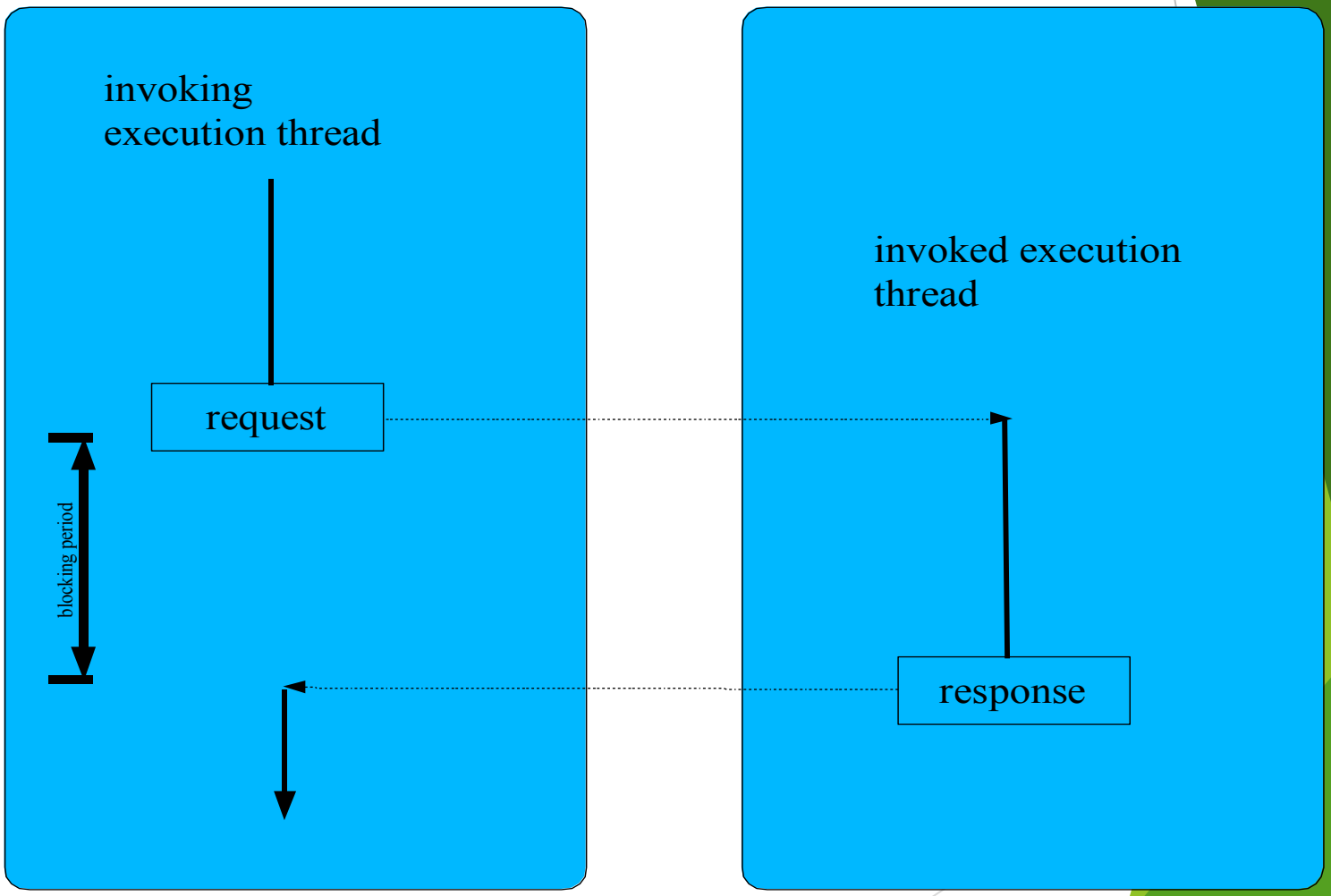
but:

- each tier increases communication costs
- complexity rises
- higher complexity of management and tuning

communication in an IS between distributed layers/tiers

- synchronous interactions
- asynchronous interactions

synchronous interactions (blocking)



asynchronous interactions (non blocking)