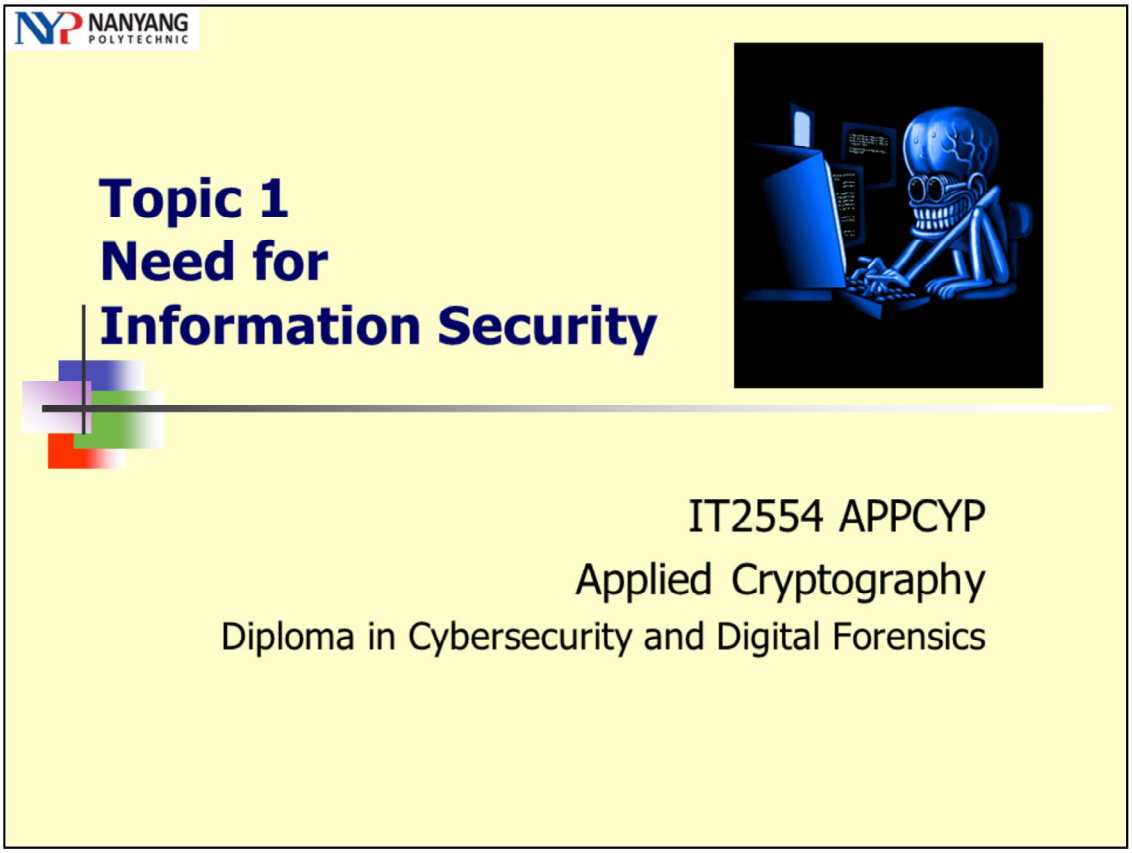
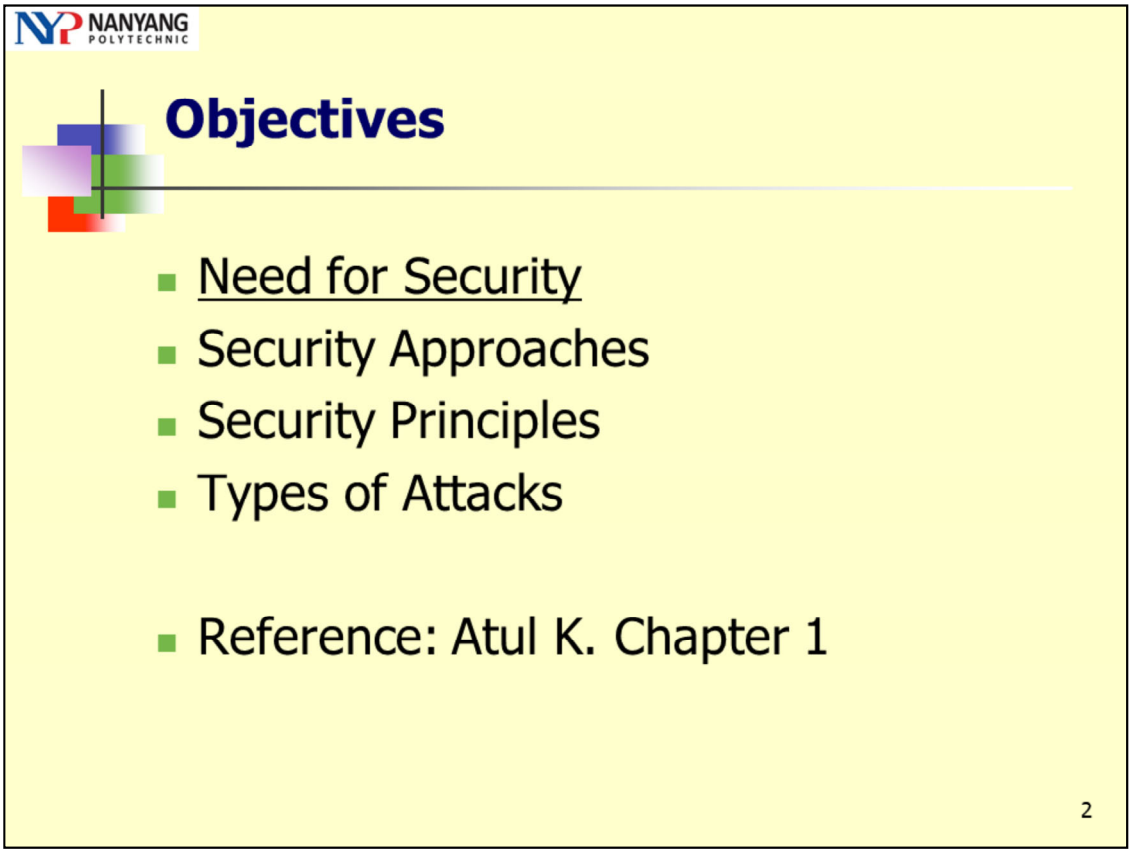


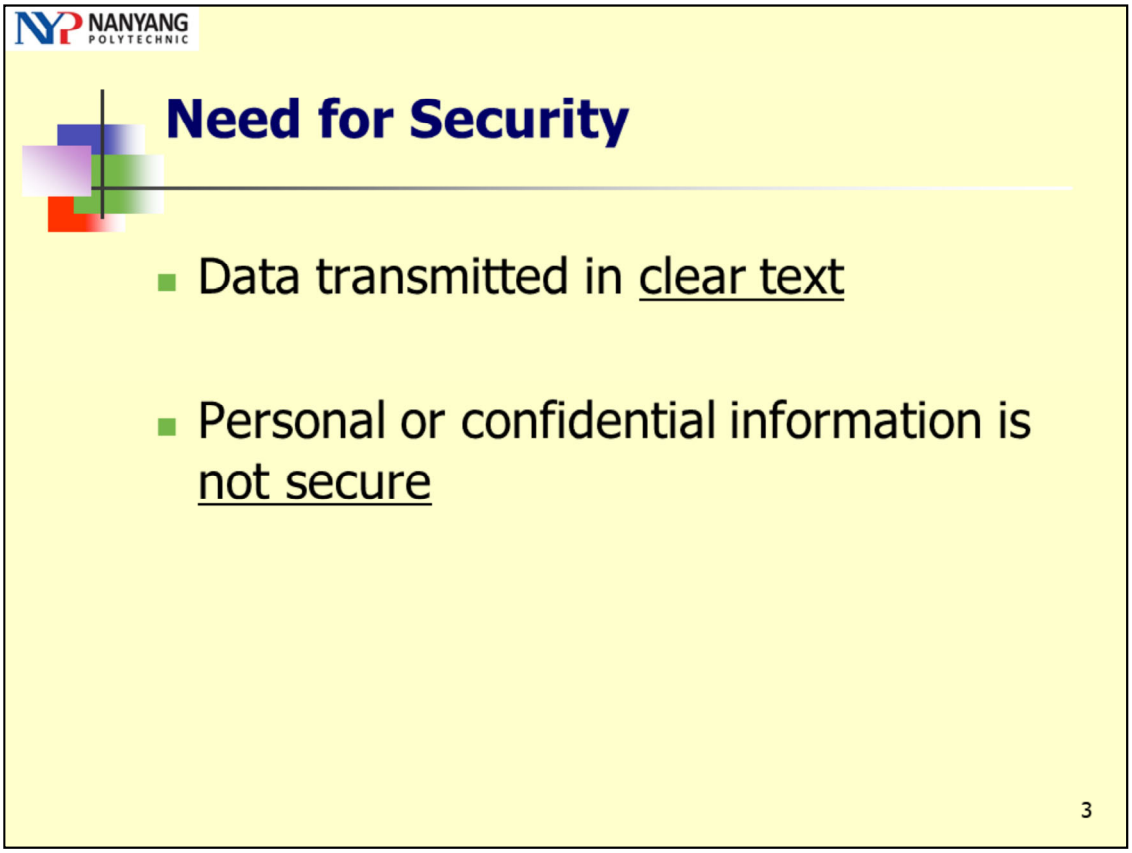
Hi, this is Topic 1 on Need for Information Security.



Objectives.

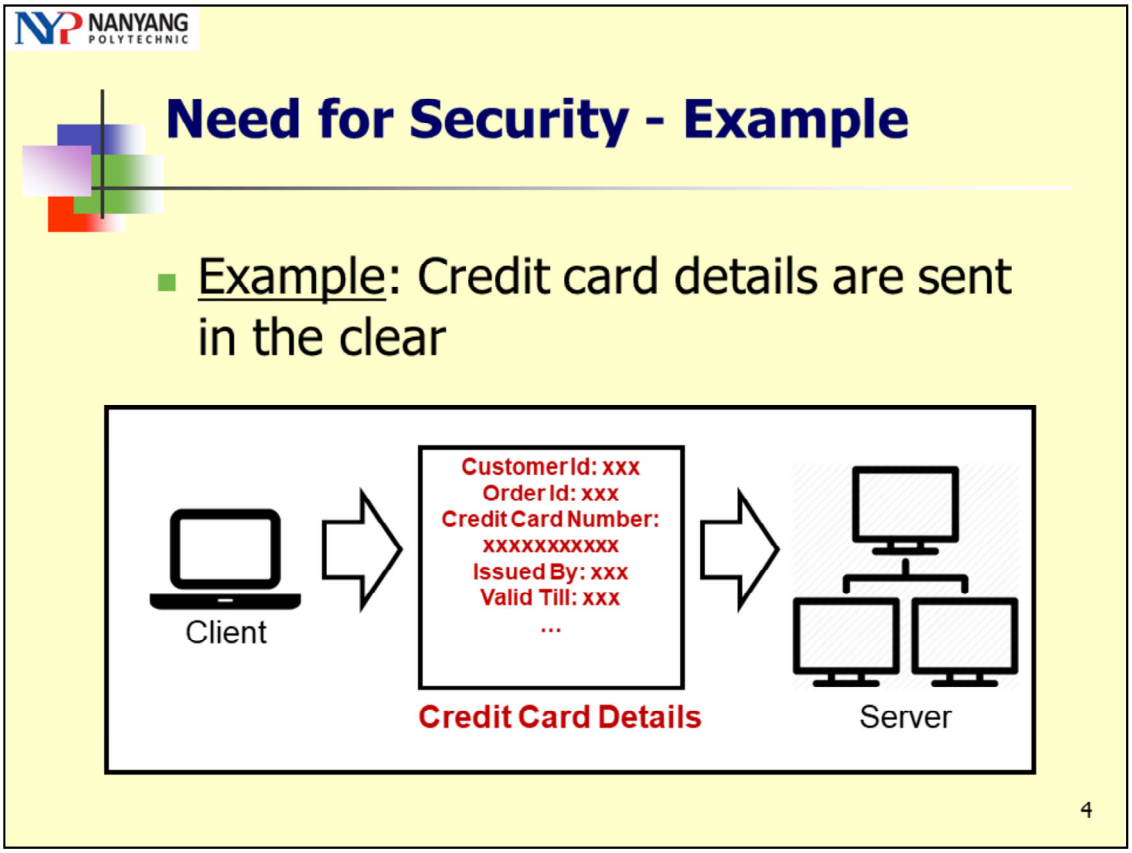
At the end of this topic, the learner will be able to:

- Describe the need for information security;
- Describe various security approaches;
- Describe some common security principles; and
- Describe some known types of computer attacks.



Need for Security.

In today's world, we use the Internet for many purposes.
We use the Internet to email our friends or colleagues,
We use the Internet to WhatsApp our families and clients,
We also use the Internet to make purchases or for banking.
If we send confidential information in the clear, i.e. unprotected,
The confidential information is not secure and can be compromised.



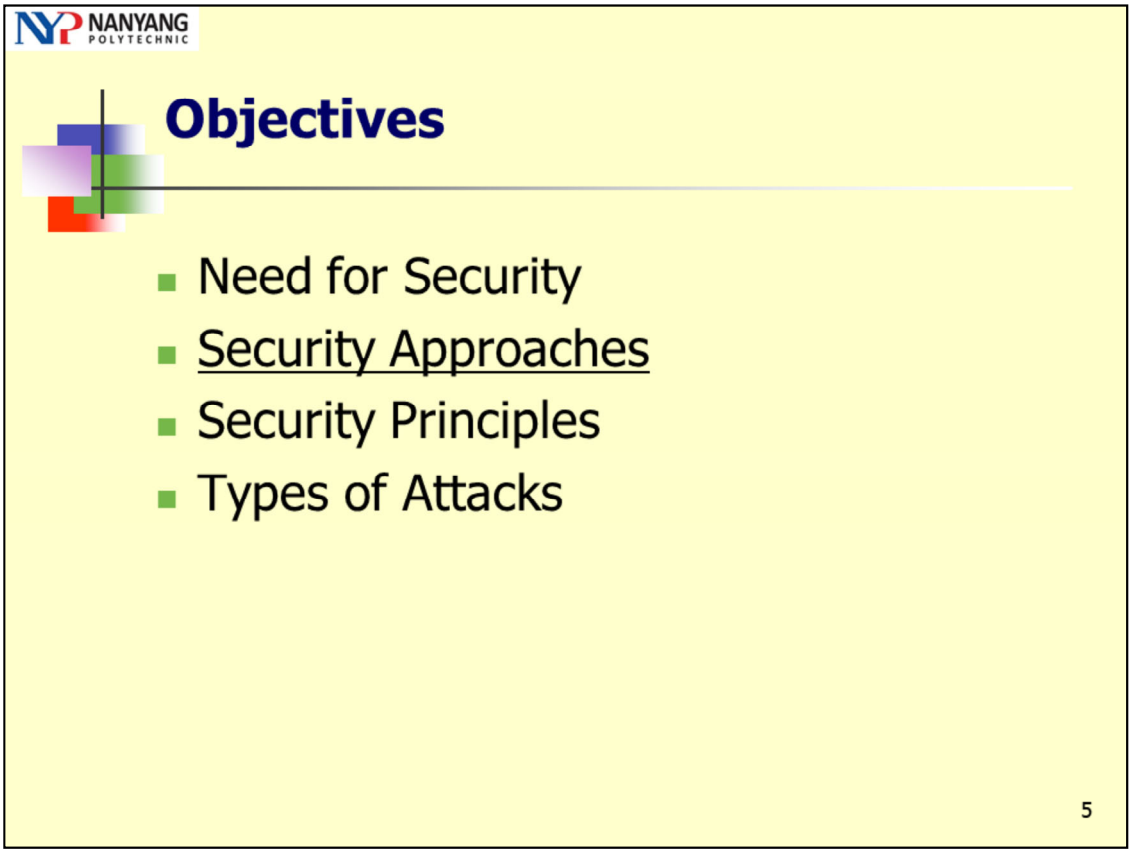
In this diagram,

If the credit card details are sent in the clear from the client to the server,

The confidential information can be compromised.

An attacker is able to sniff the communication channel,

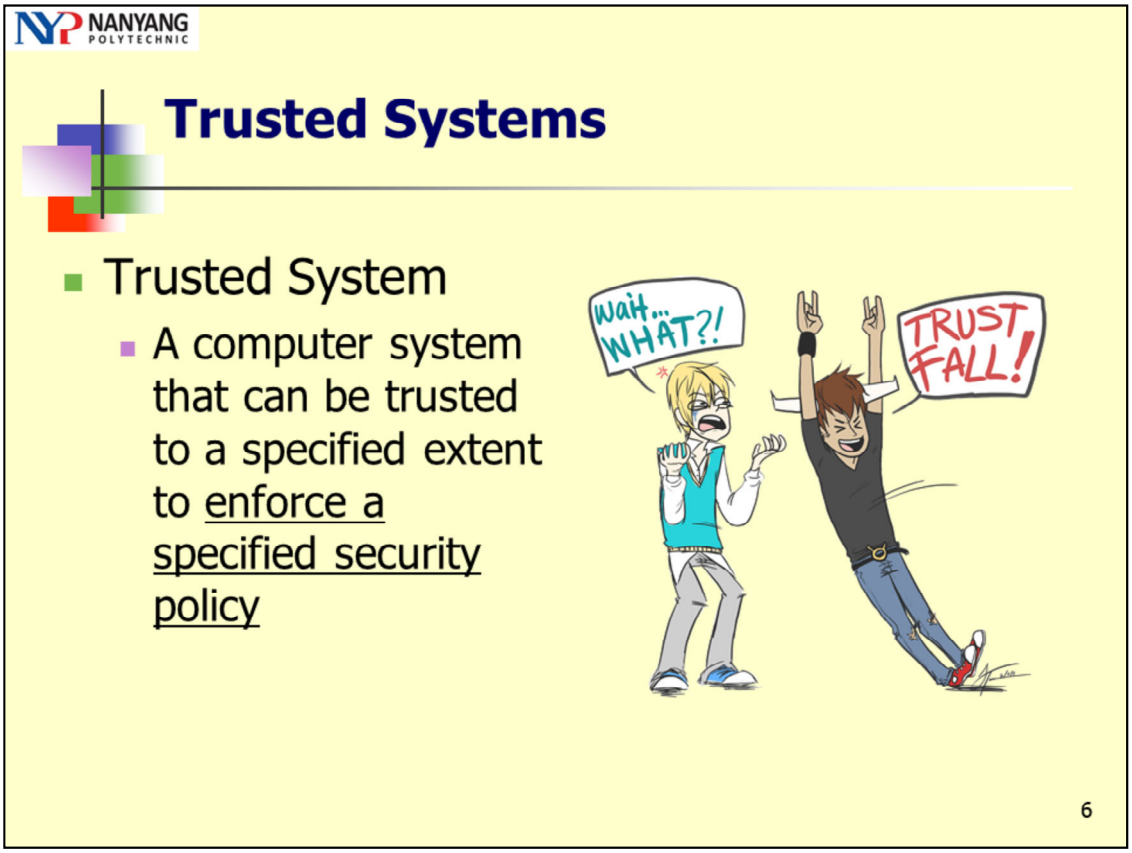
And read the credit card details.



Security Approaches.

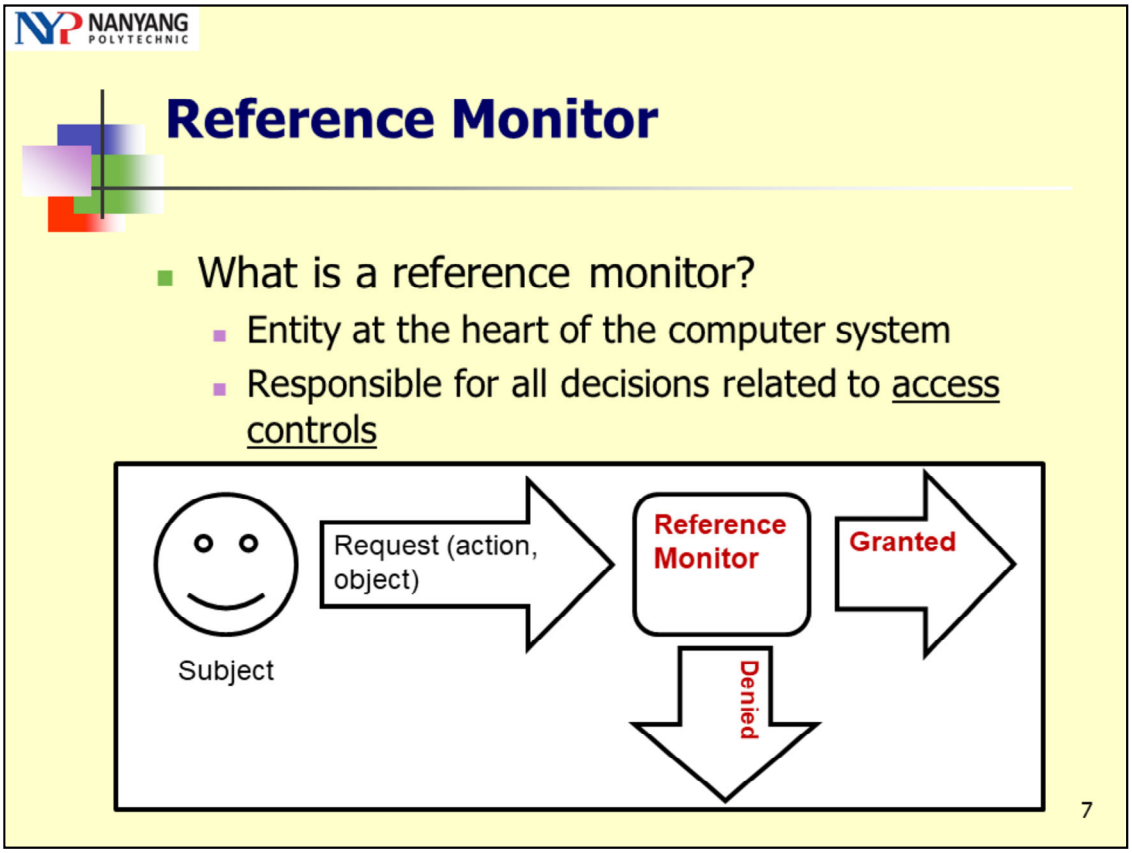
In this section, we'll learn:

- What is a trusted system;
- What is a reference monitor;
- 4 approaches to implement a security model; and
- 4 key characteristics of a security policy.



What is a trusted system?

A trusted system is a computer system that can be trusted to a specified extent. It is able to enforce a specified security policy.



Reference Monitor.

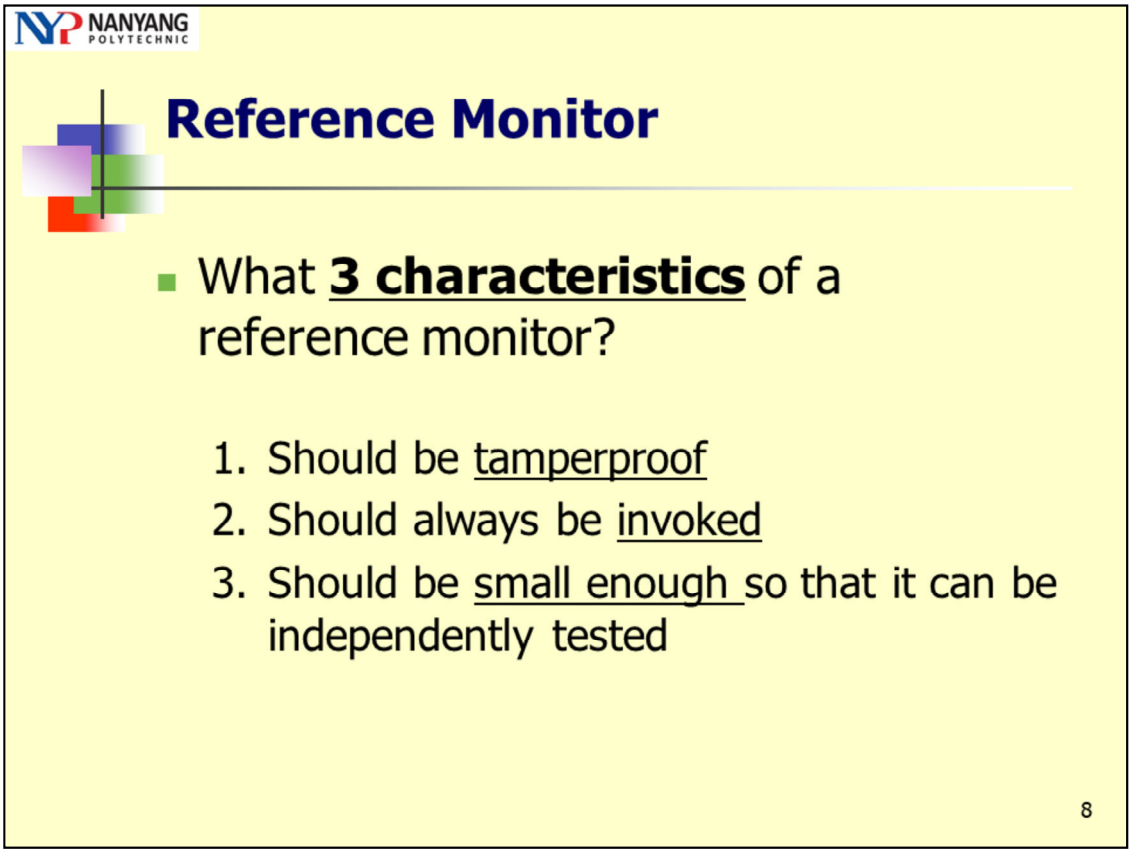
A trusted system can be implemented using a reference monitor.

What is a reference monitor?

A reference monitor is an entity at the heart of a computer system.
It is responsible for all decisions related to enforcing access controls.

Suppose a subject would like to request for an action on an object,
The reference monitor will check the request to determine if the subject has the privilege to do so.
If he has, access is granted. If not, access is denied.

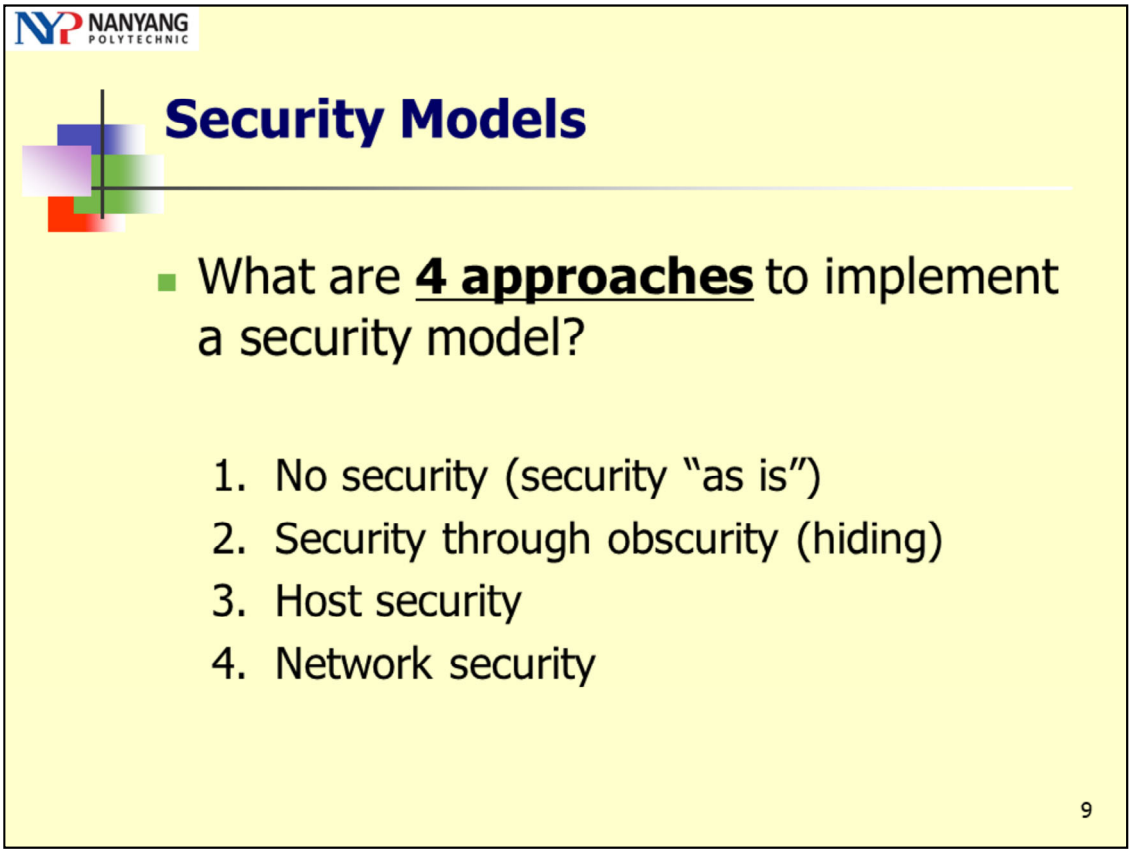
For example, if a user requests to read a file,
The reference monitor will check if the user has read access to the file.
If he has, access is granted. If not, access is denied.



For a reference monitor to be effective,

It has to satisfy 3 characteristics:

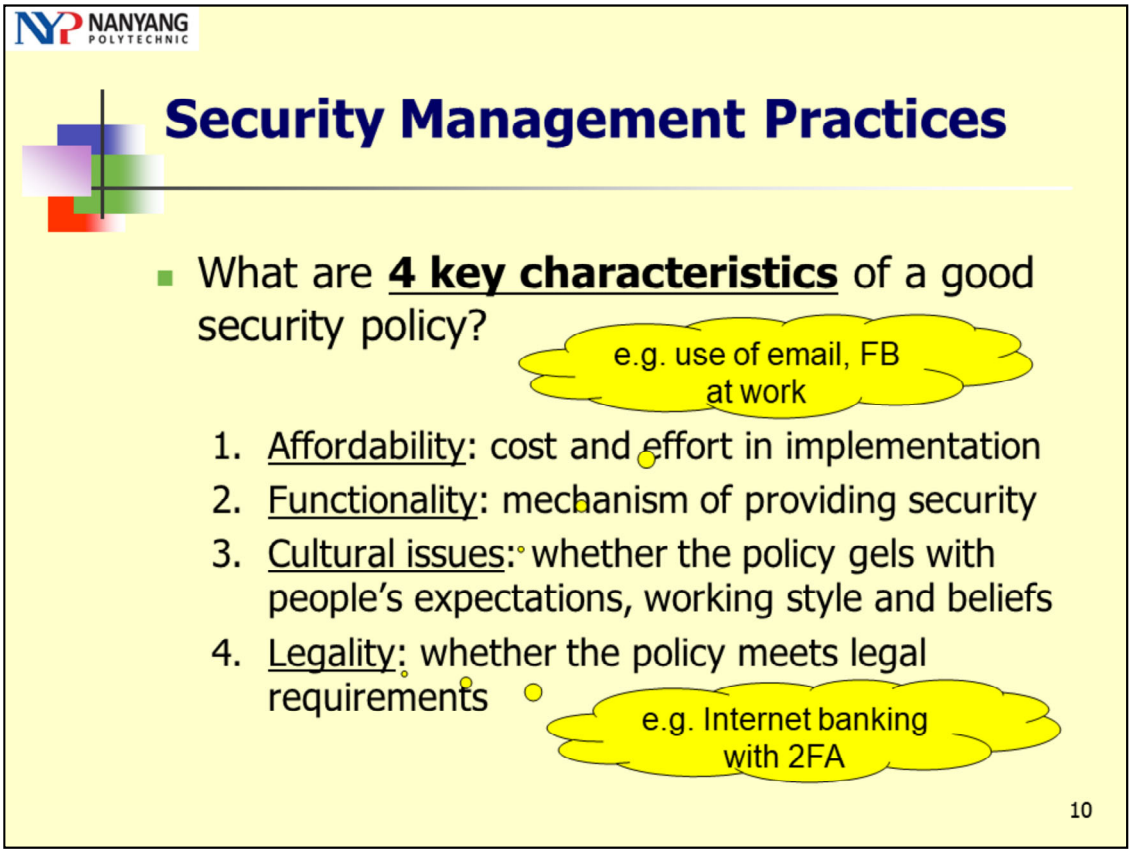
- It should be tamperproof, e.g. if is not compromised;
- It should always be invoked, so that it is able to enforce all requests; and
- It should be small enough, so that it can be independently tested.



Security Models.

There are 4 approaches to implement a security model.

- In "no security",
  - We use the system "as is" or "out of the box";
  - We use the system with the default security configuration; and
  - We do not need to use additional security protection.
- In "security through obscurity",
  - We secure confidential information by hiding them.
- In "host security",
  - We provide security by protecting the host;
  - E.g. we can provide user authentication and access control.
- In "network security",
  - We protect the network;
  - E.g. we can encrypt the communication channel.

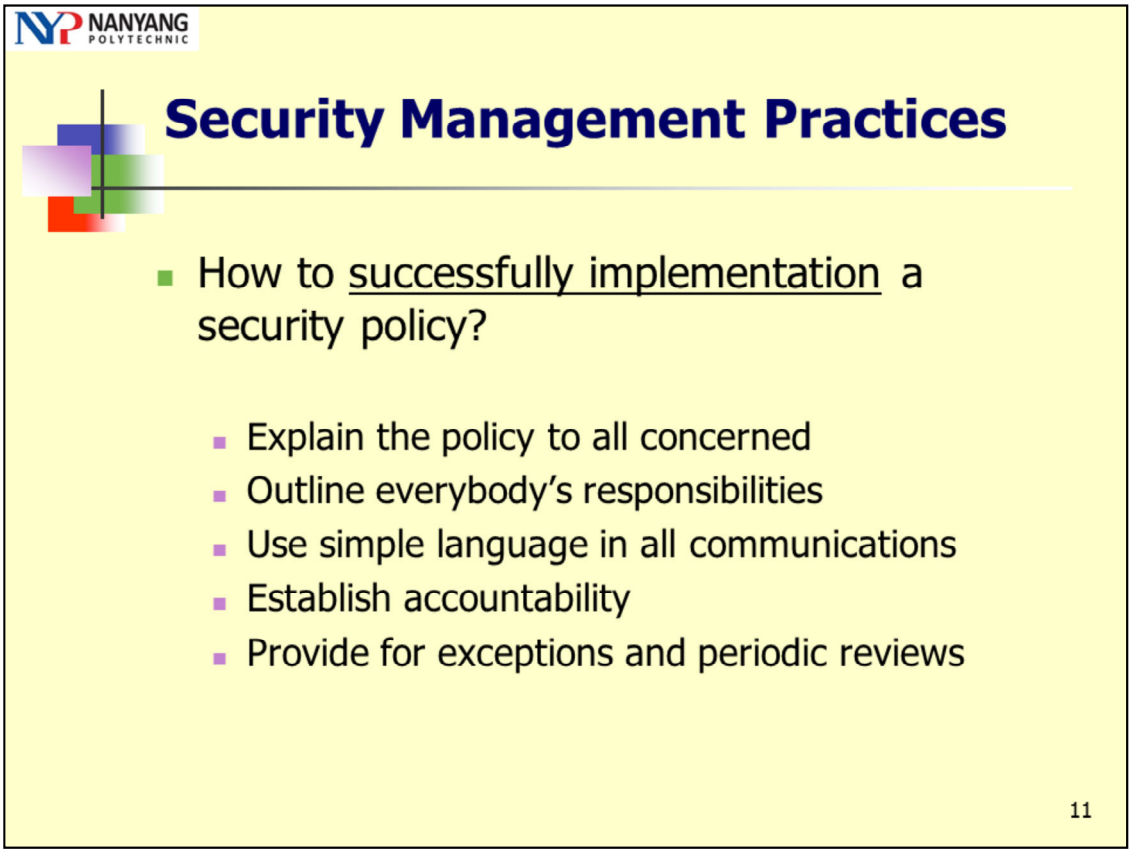


Security Management Practices.

There are 4 key characteristics of a good security policy:

1. Affordability: the security policy should not be too costly and incur too much effort to implement;
2. Functionality: there should be available security mechanism to support the security policy;
3. Cultural issues: the security policy should gel with people's expectations, working style and beliefs;
    - e.g. in the use of email, WhatsApp and Facebook at work; and

4. Legality: the policy should meet legal requirements.
    - e.g. use of 2FA in Internet banking.

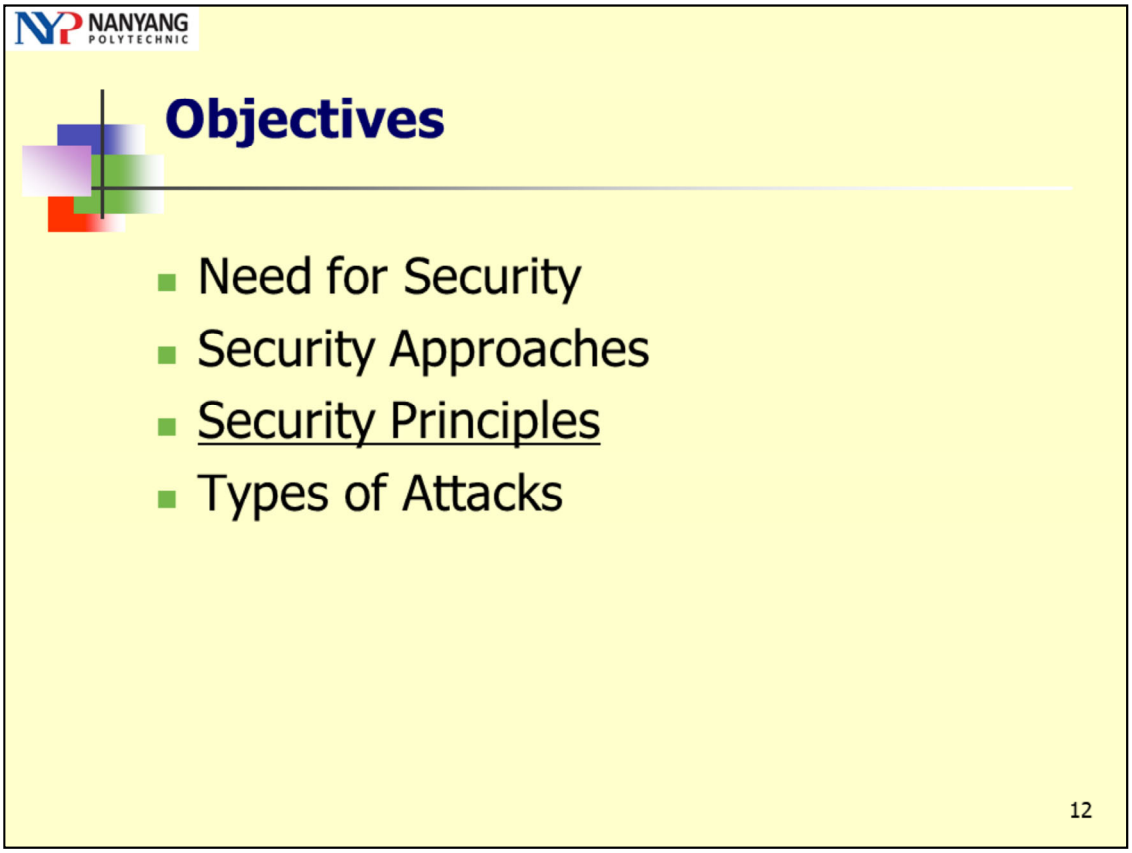


Security policy is mandatory and needs to be successfully implemented.

How to successfully implement a security policy?

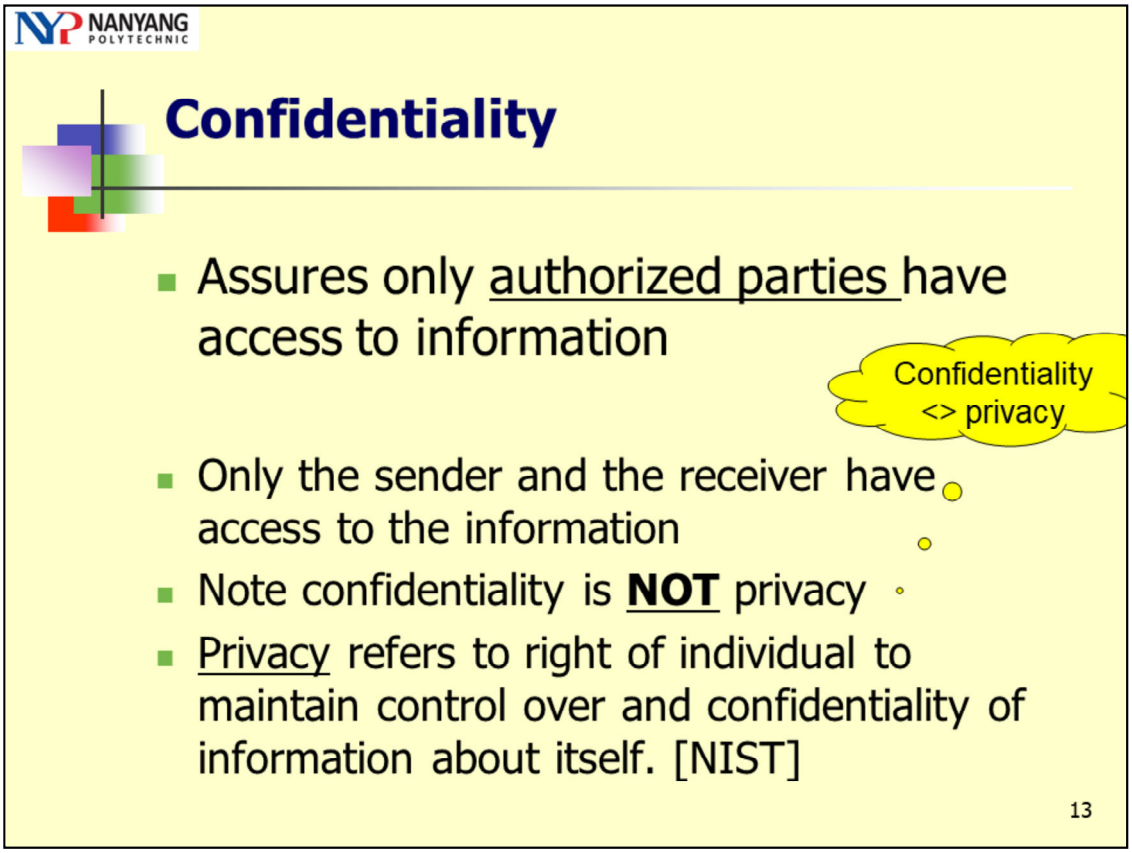
It can be done in the following ways:

- Explain the security policy to all concerned, so that
    - The relevant stakeholders understand the need for the policy; and
    - We are able to get their buy-in.
- Outline everybody's responsibilities, so that
    - All relevant stakeholders know what and how they are protecting the information.
- Use simple language in all communications, so that
    - All relevant stakeholders understand the policy without doubts.
- Establish accountability, so that
    - All relevant stakeholders know what they are accountable for.
- Provide for exceptions and periodic review, so that
    - The policy can be continuously updated and improved.



In this section, we'll learn:

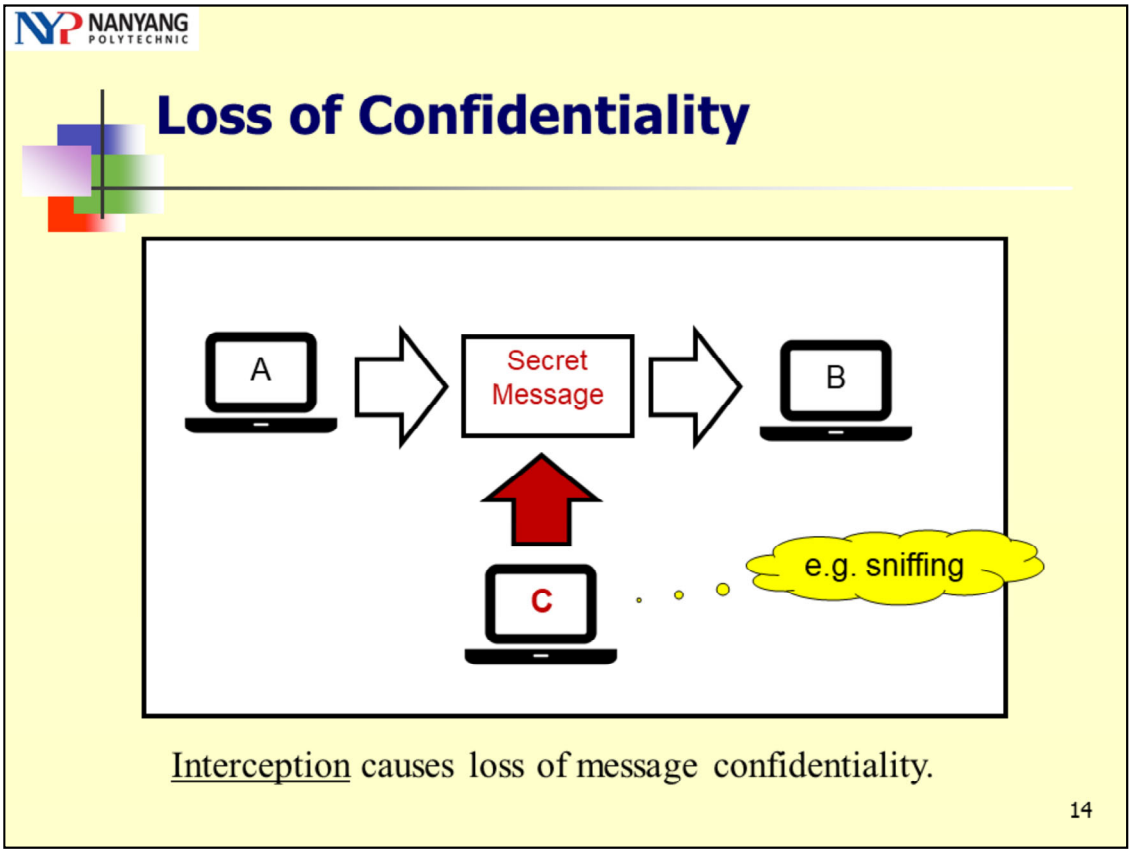
- The security principles related to confidentiality, authentication, integrity, non-repudiation, access control and availability; and
- The attacks on these security principles.



The first security principle is confidentiality.
It assures only authorized parties have access to information,
While unauthorized parties will not have access to information.

Suppose party A wants to send a confidential message to party B,
Only party A and party B have access to the message.
Other parties should not have access to the message.

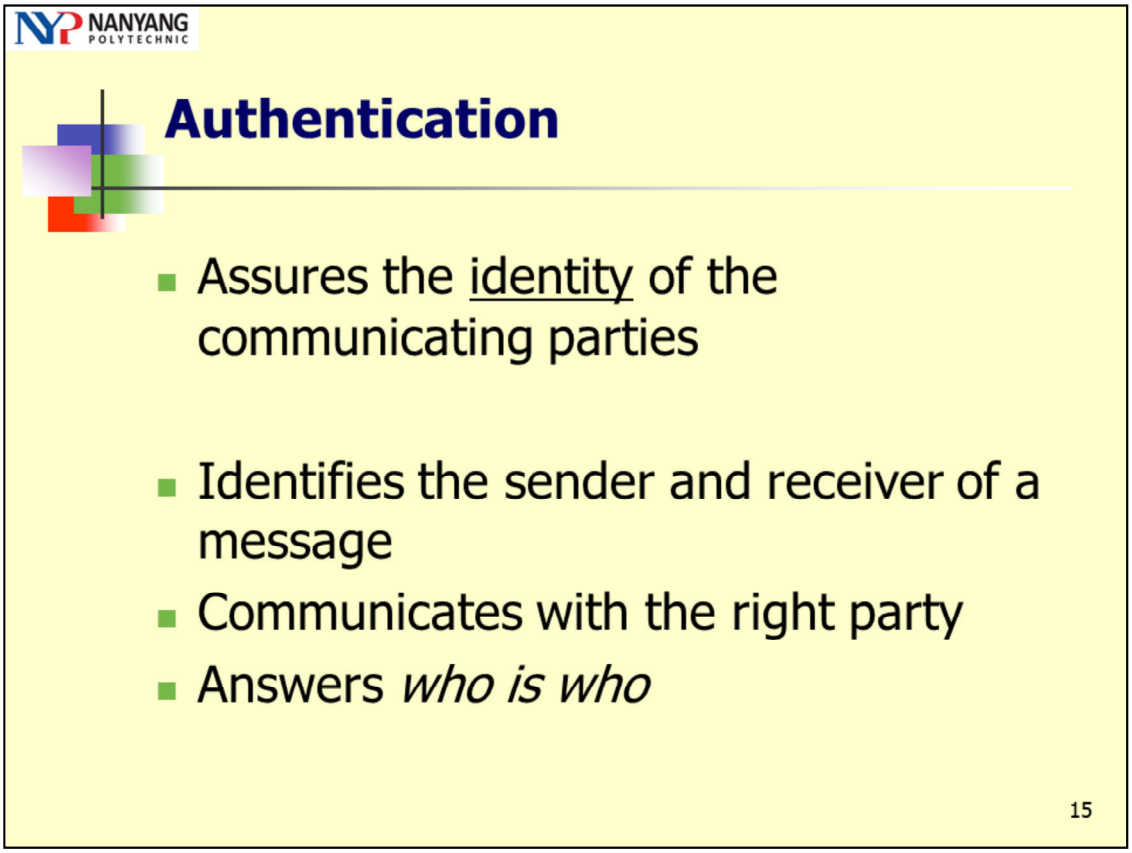
Note that confidentiality is different from privacy.
Privacy refers to the right of an individual
To maintain control over and confidentiality of information about itself.



Confidentiality can be compromised by interception.

In this example,
Suppose party A sends a secret message to party B.
Party C can intercept the message by sniffing the network
To gain unauthorized access to the secret message.

A solution to loss of confidentiality is to use encryption/decryption.
This will be covered in subsequent session.



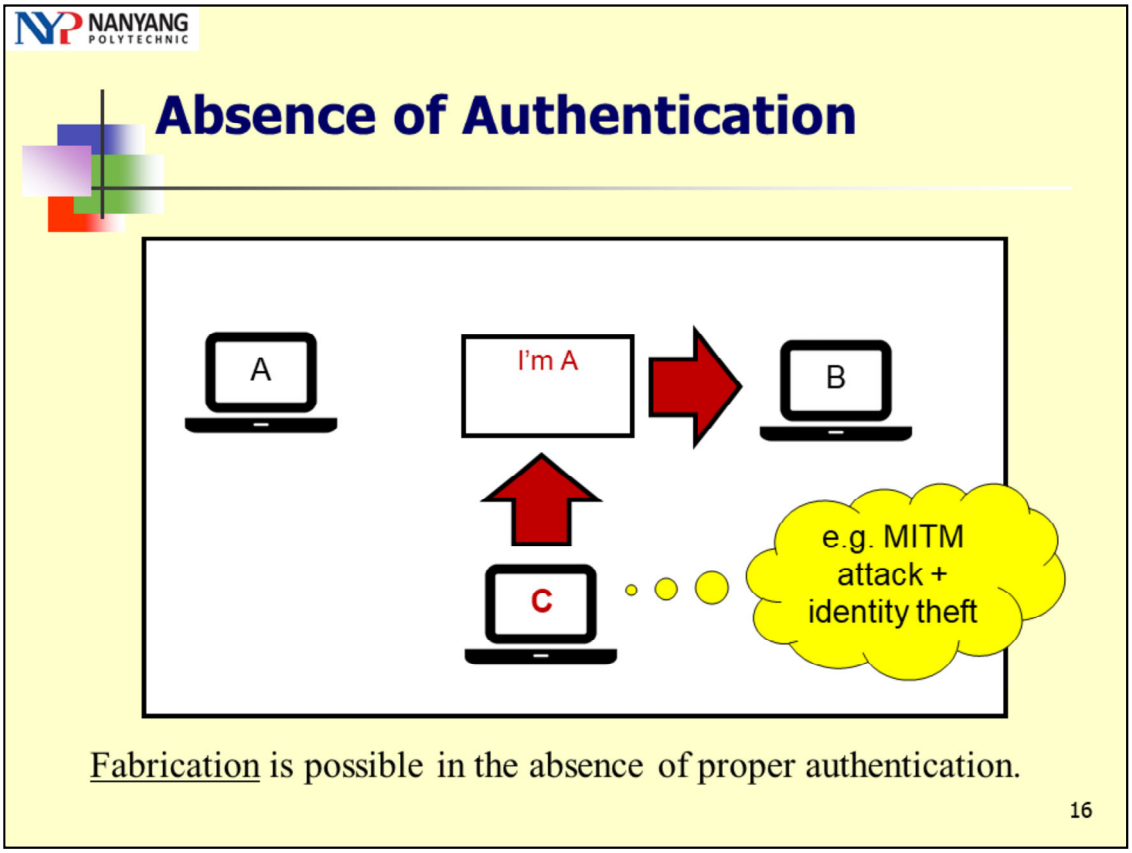
The next security principle is authentication.

Authentication assures the identity of the communicating parties.

Suppose party A would like to communicate with party B.

Party A would like to be assured that party B is indeed party B.

In other words, party B is who he claims he is.



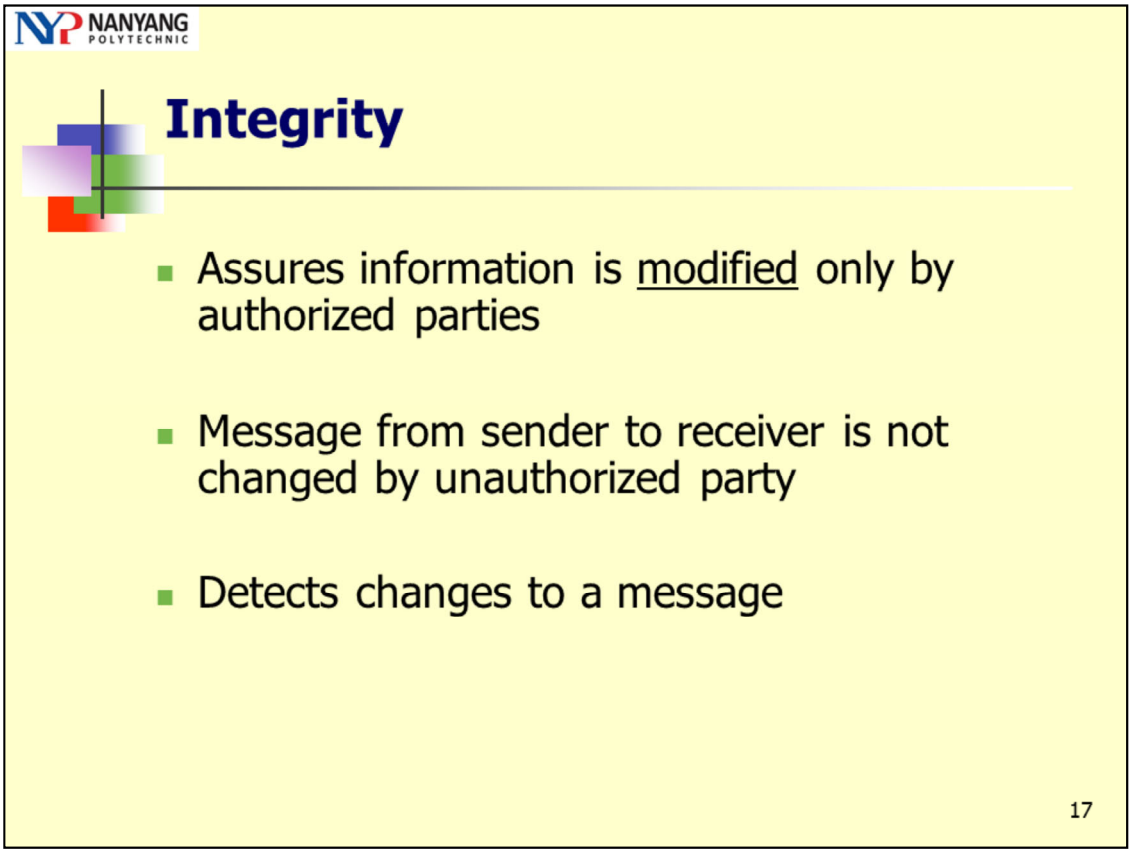
Authentication can be compromised by fabrication.

Suppose party A and party B trust each other.
Party C can launch a man-in-the-middle, aka MITM, attack
To steal the identity of party A and
Pretend to be party A and communicate with party B.
This is an example of identity theft.

Authentication can be provided by one or more of the following methods/factors:

- Based on what you know, e.g. user ID and password;
- Based on what you have, e.g. security token; and
- Based on what you are, e.g. fingerprint and retina characteristic.

Using 2 of the above 3 methods is called 2-factor authentication, 2FA in short.



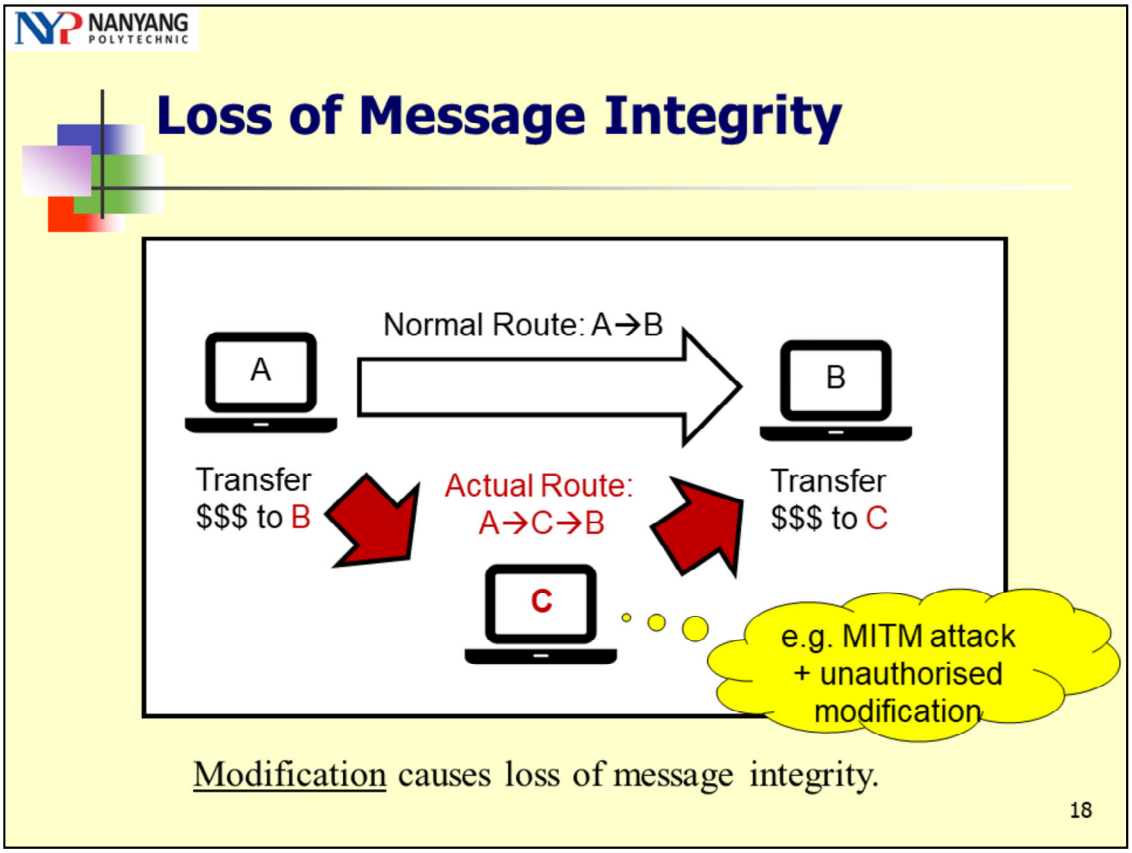
The next security principle is called integrity.

Integrity assures information is modified only by authorized parties.

If party A sends a message to party B,

The message should not be changed by an unauthorized party in transit.

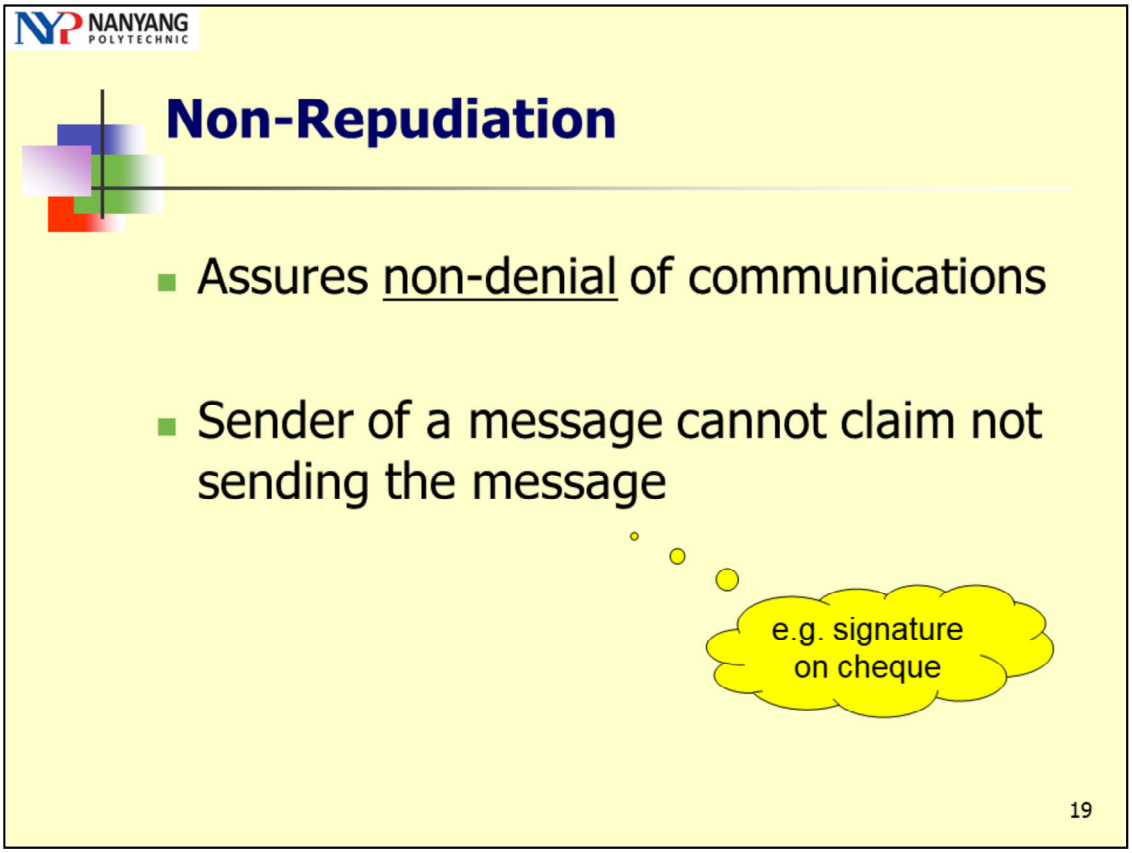
Integrity can be used to detect unauthorized changes to a message.



Modification can be used to compromise message integrity.

In this example,
Suppose party A is communicating with party B.
Party A sends an instruction to “transfer money to party B”.
Party C can launch a MITM attack
To perform an unauthorized modification to the message
And modify the message to “transfer money to C”.
This leads to loss of message integrity.

A countermeasure against loss of message integrity is to use a hash function.
This will be covered in subsequent session.

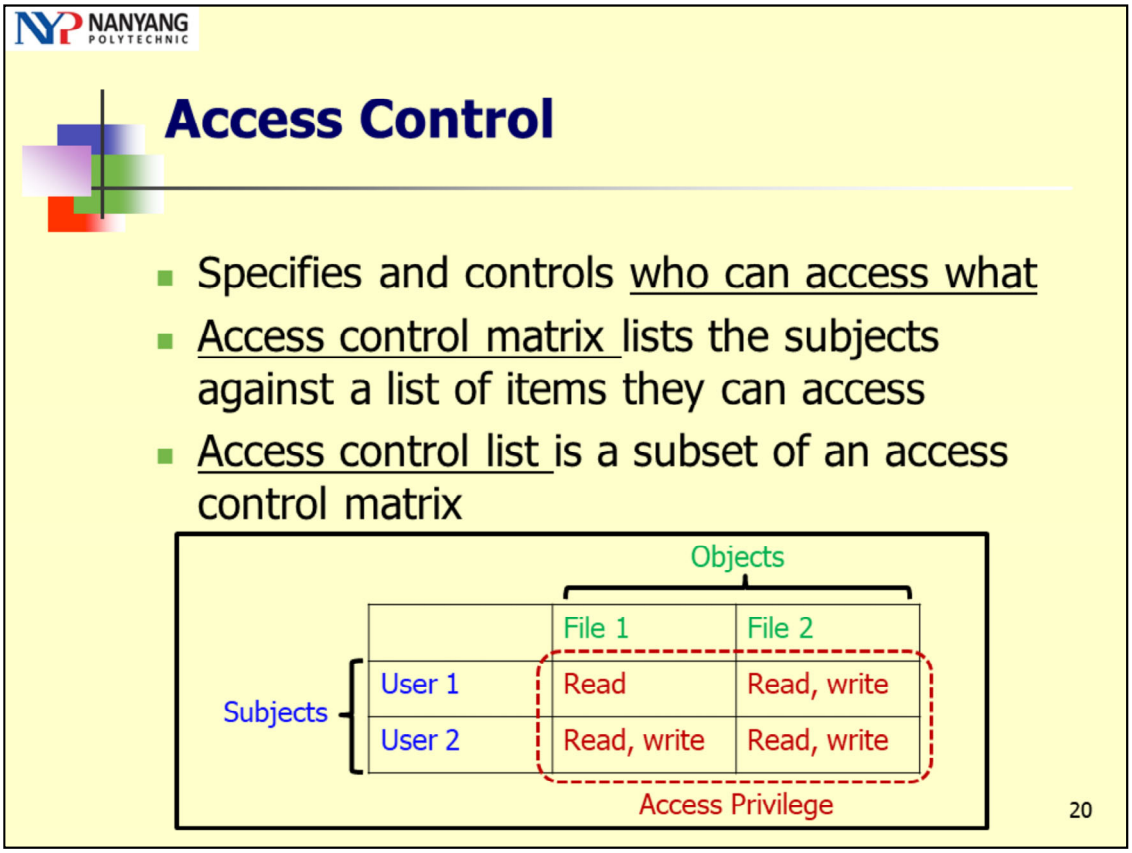


Another important security principle is non-repudiation.
This assures non-denial of communications.

Suppose party A sends a message to party B,
Party A should not be able to deny not having sent the message.

In the example of a paper cheque,
Suppose party A signs a cheque for a payment to party B,
Party A should not be able to deny not have made the payment,
As he had signed on the cheque.

Non-repudiation can be provided by the use of digital signature.
This will be covered in subsequent session.



Another security principle is called access control.

Access control assures a subject is granted the access privilege to the objects he is granted access.

In this example,

User 1 is granted read access to File 1 as well as read and write access to File 2,

While user 2 is granted read and write access to both File 1 and File 2.

Access control can be implemented by using an access control matrix or an access control list.

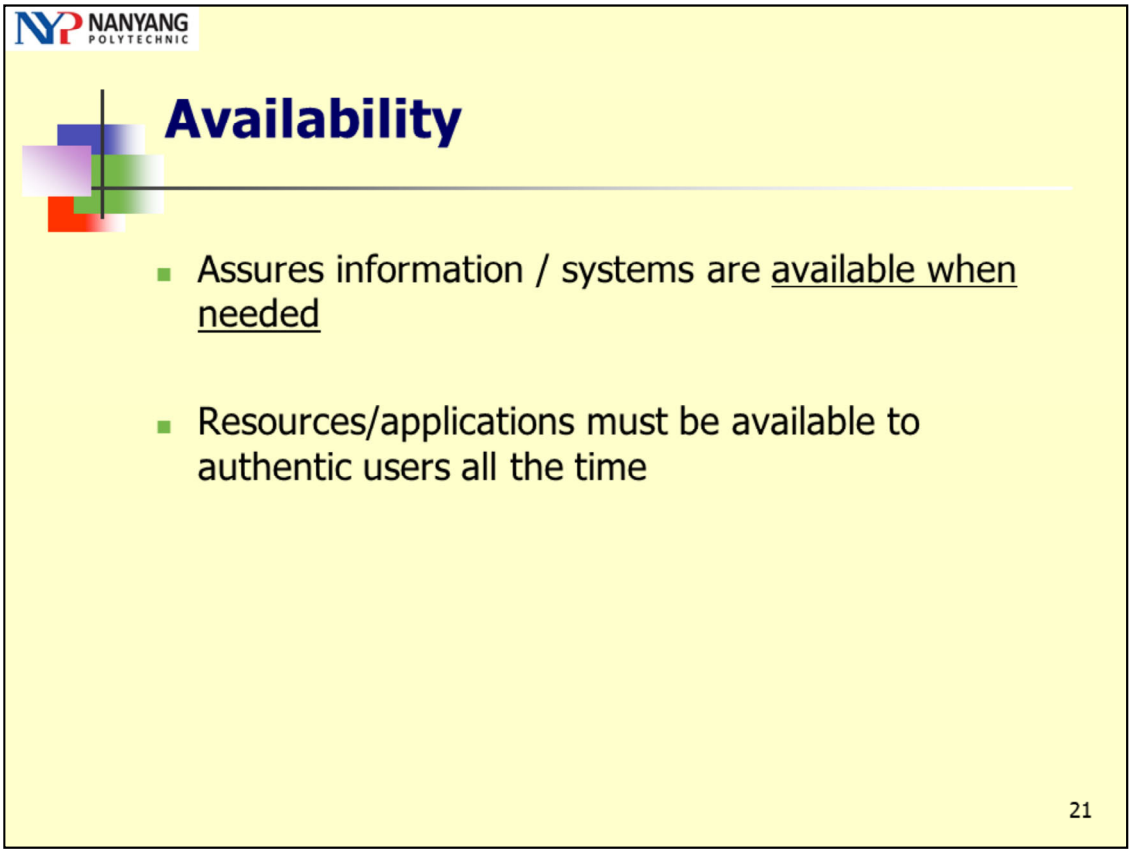
The diagram shows an example of an access control matrix.

It lists the subjects against a list of objects which the subjects can access and the corresponding access privileges.

Each row is called an access profile for the subject,

Whereas each column is called the access control list for the object.

Reference: RFC 4949.

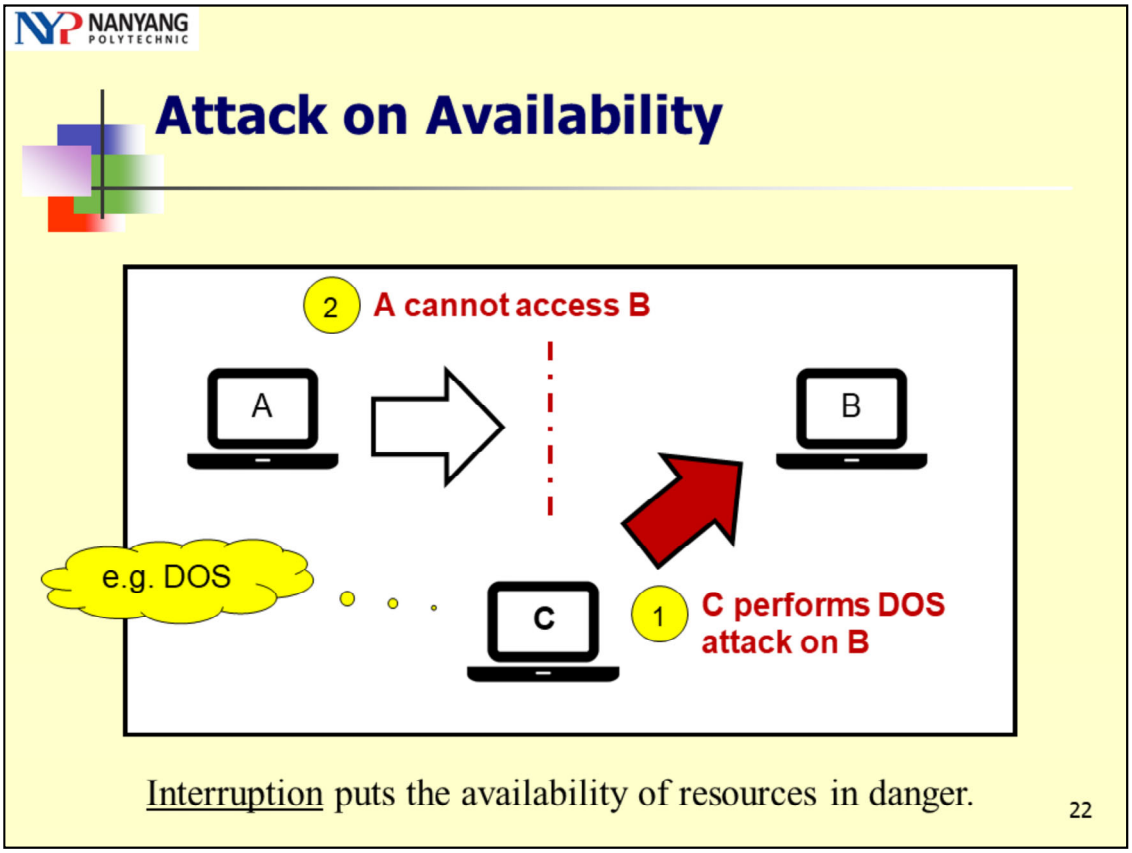


The last security principle of interest here, but certainly not the least, is availability.

Availability assures information/systems are available when needed.

In other words, the information/systems are there in a timely fashion

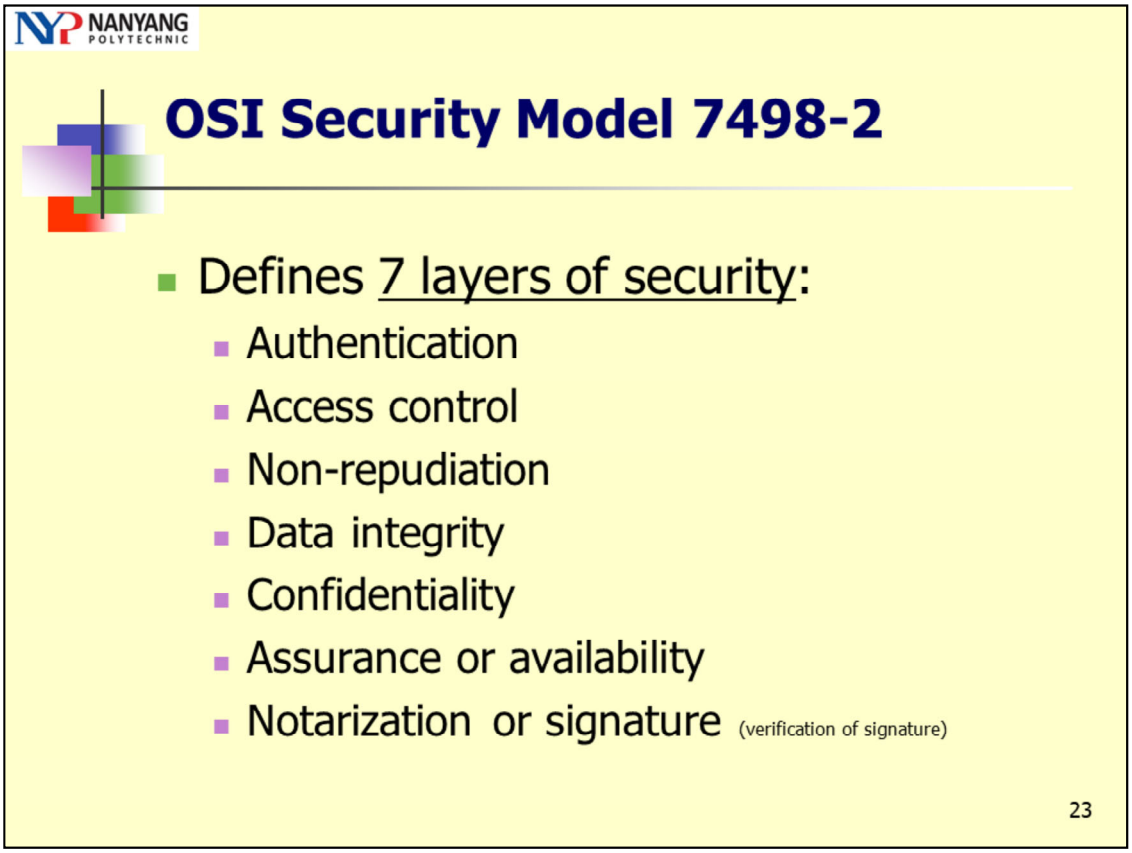
When we need to access them.



Interruption can be used to compromise availability.

In this diagram,
Suppose party A would like to access party B.
However, party C can launch a denial-of-service (DOS) attack on party B.
The DOS attack brings party B down and makes it inaccessible by party A.

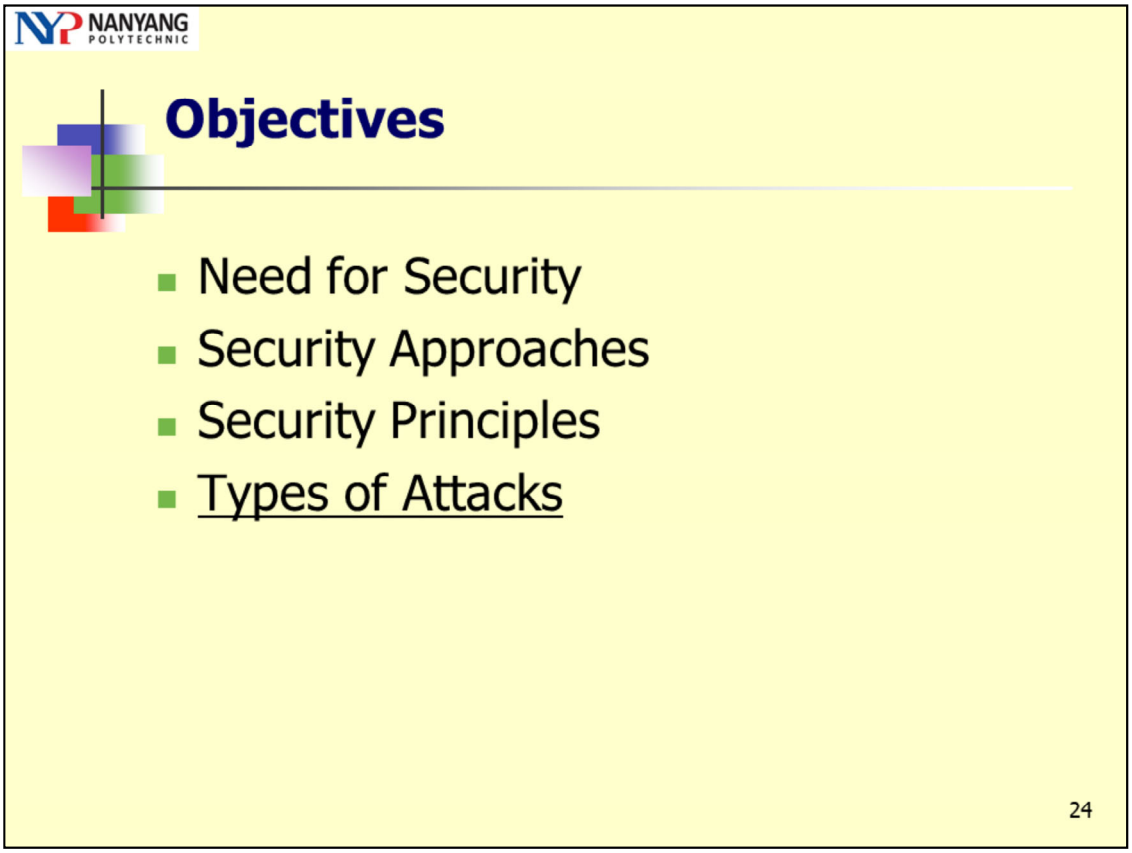
Countermeasures against interruption includes
Increasing network bandwidth, providing system and network redundancy, etc.



For more information on security principles,

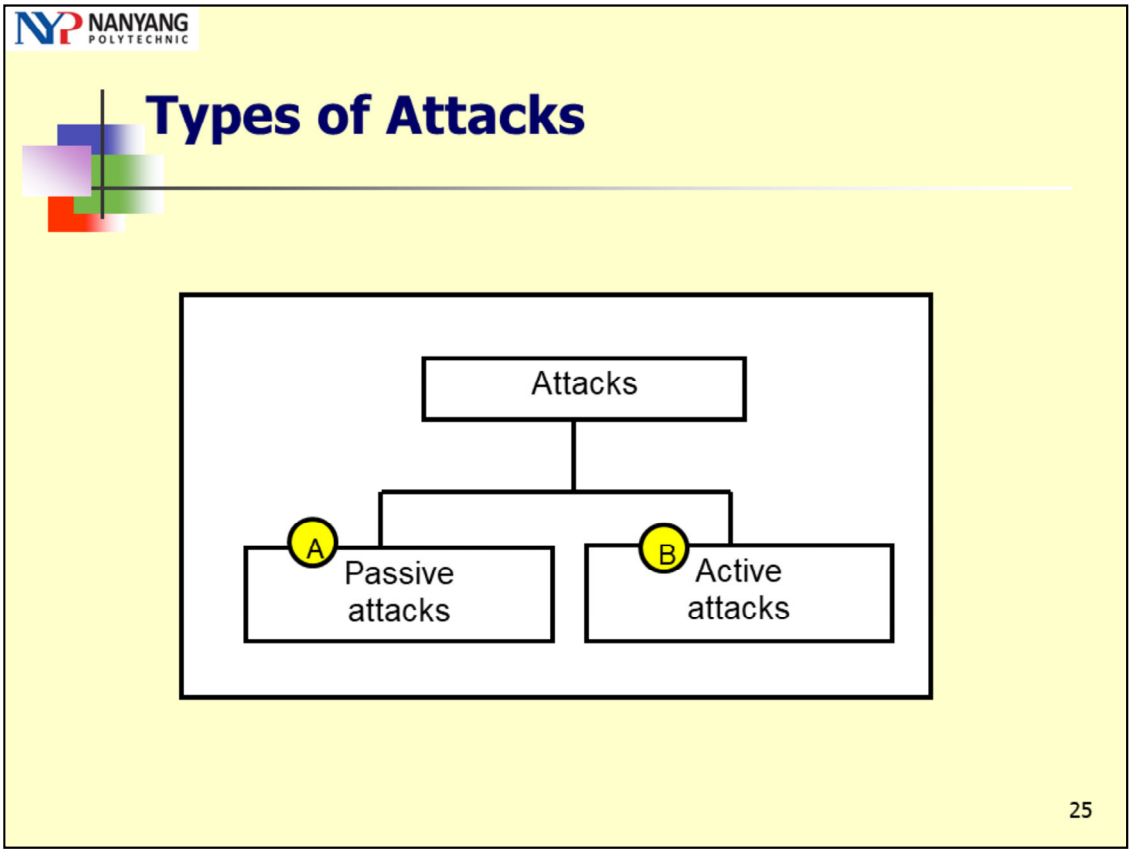
Refer to OSI Security Module 7498-2,

Which defines 7 layers of security.

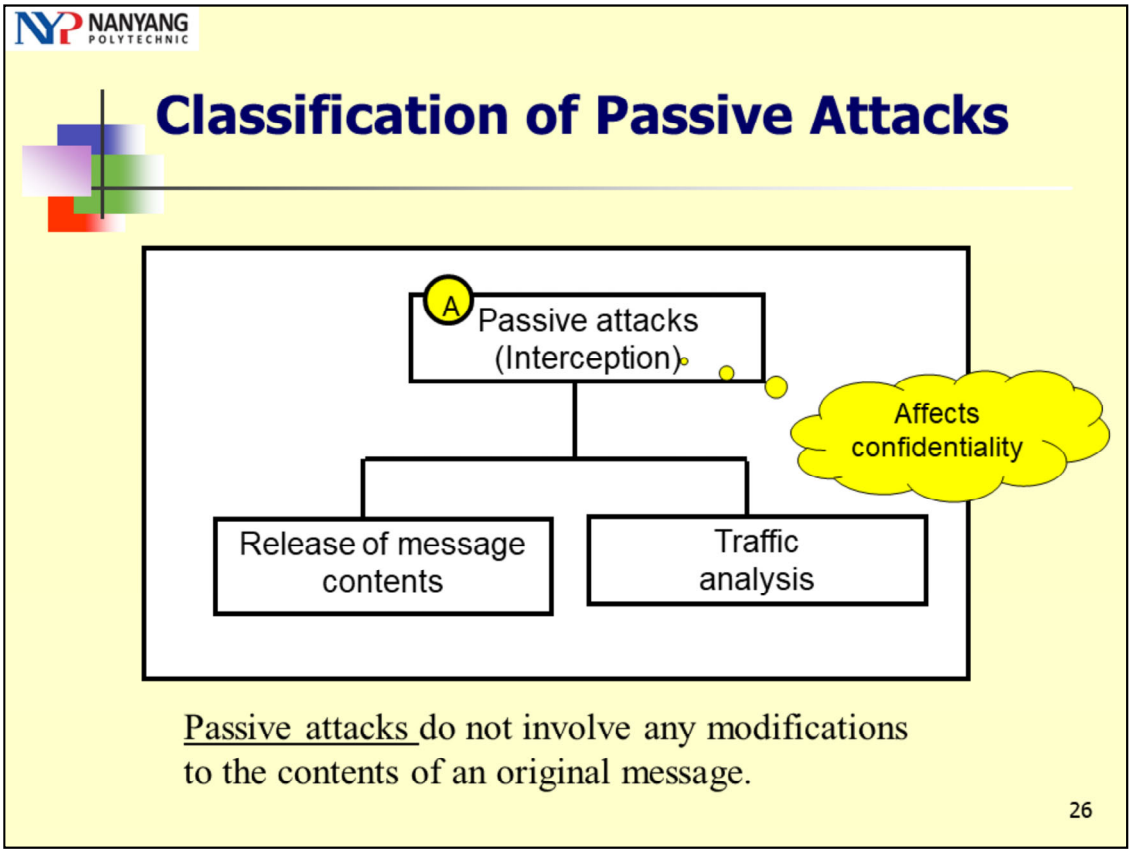


There many ways to classify different types of attacks.

In this section, we shall learn one classification.



Attacks can be classified as passive attacks or active attacks.



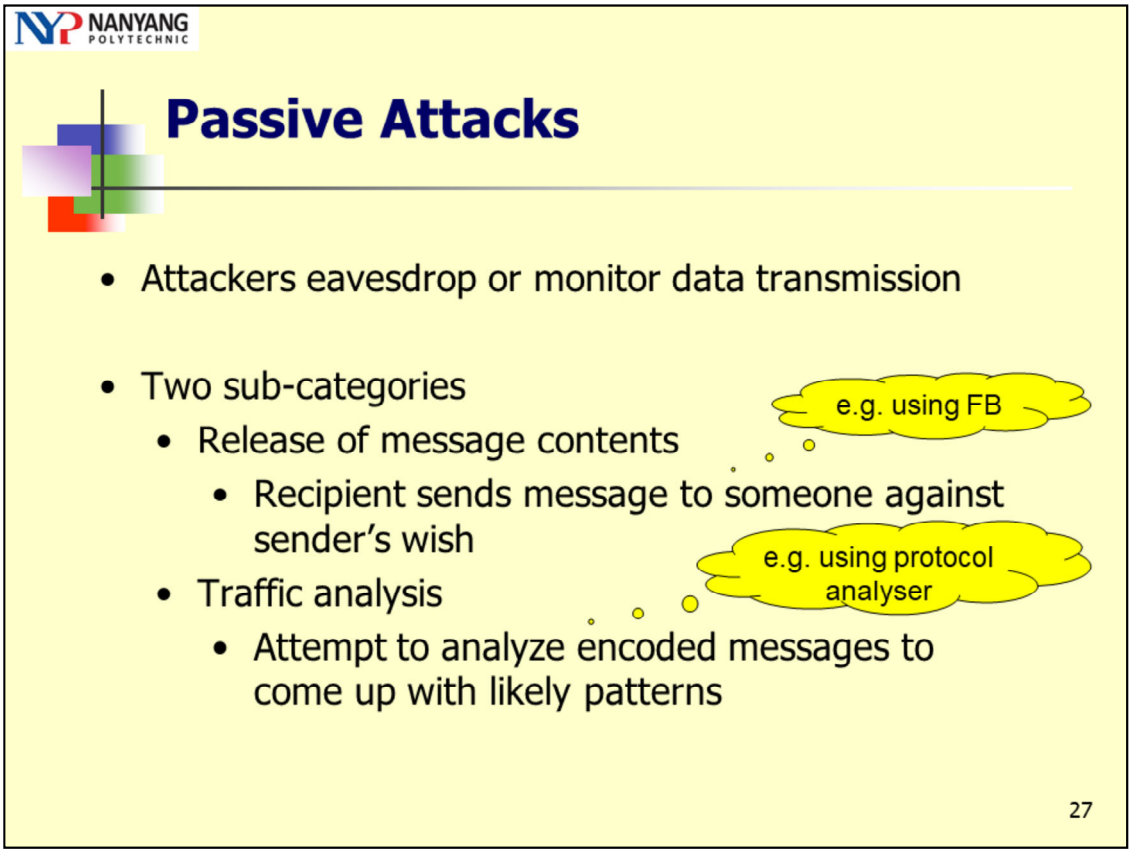
A passive attack does not involve any modifications to the contents of an original message.

It can be an interception to a message,

Which affects the message confidentiality.

There are 2 types of passive attacks, namely:

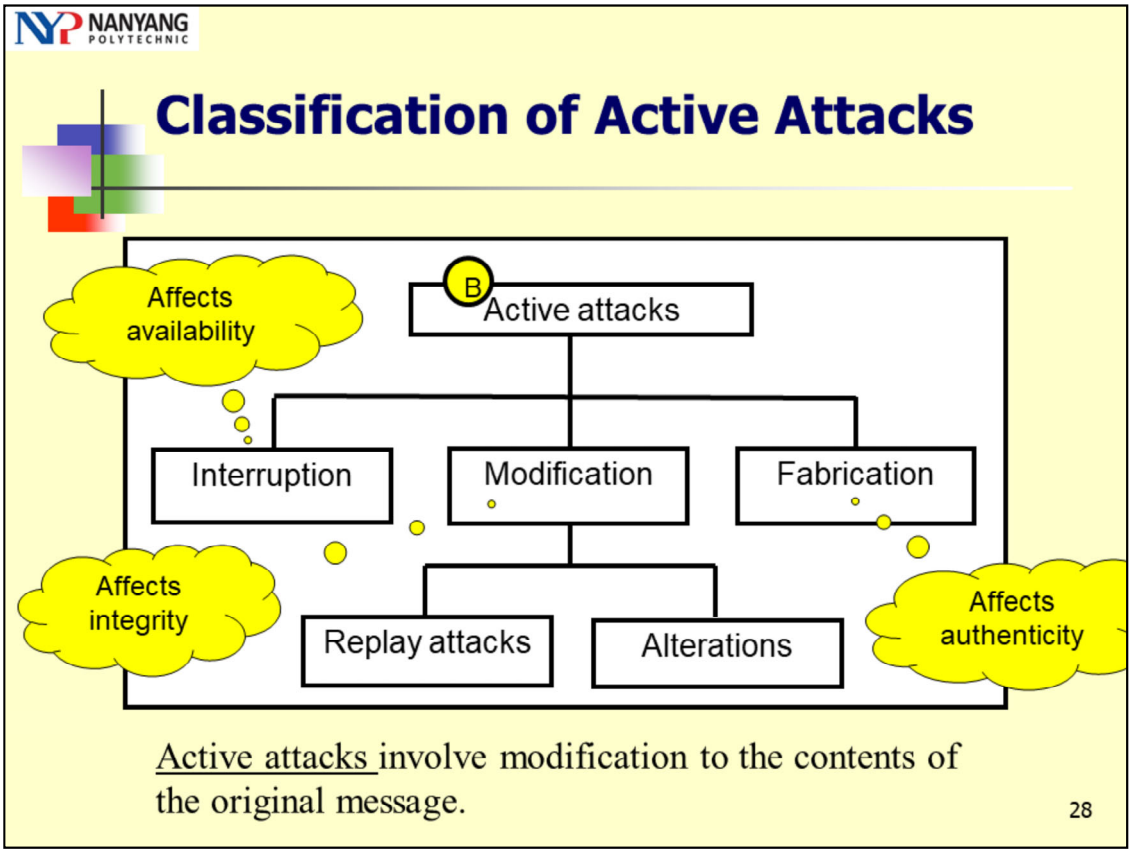
- Release of message contents; and
- Traffic analysis.



A passive attack typically involves eavesdropping or monitoring of data transmission.
For instance, an attacker compromises data confidentiality
By performing unauthorized sniffing of data in a communication channel.

There are 2 sub-categories of passive attacks:

- In release of message contents attack,
    - The recipient of a message can be an attacker.
    - He sends the message to someone against the sender's wish,
    - e.g. in a Facebook post.
- On the other hand, in traffic analysis attack,
    - The attacker sniff the network; and
    - Attempt to analyse the encoded messages to make sense out of them,
    - e.g. by using a protocol analyser.



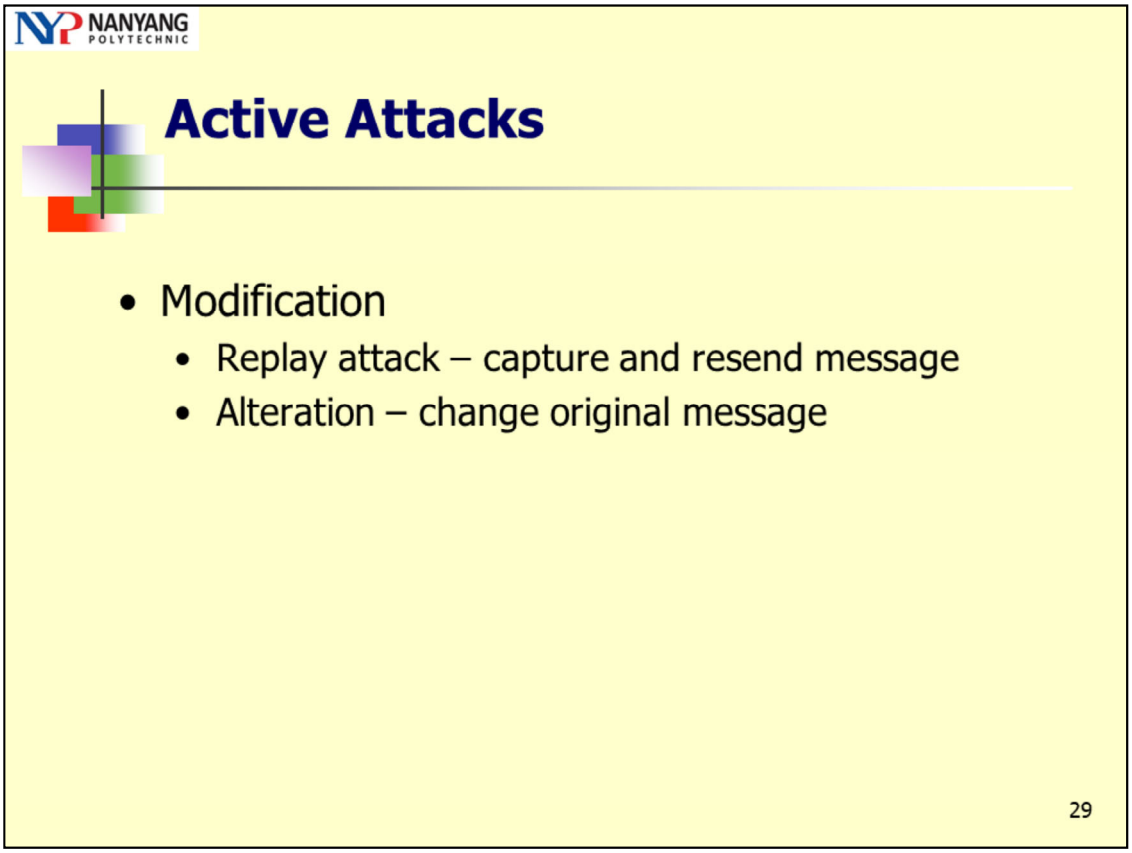
In contrast to a passive attack,

An active attack involves modification to the contents of the original message.

There are 3 sub-categories of active attacks:

- Interruption attack affects the availability of information/system;
- Modification attack affects the integrity of a message; and
- Fabrication attack affects the authenticity of the communication.

Modification attacks can in turn be divided into replay attacks and alterations.

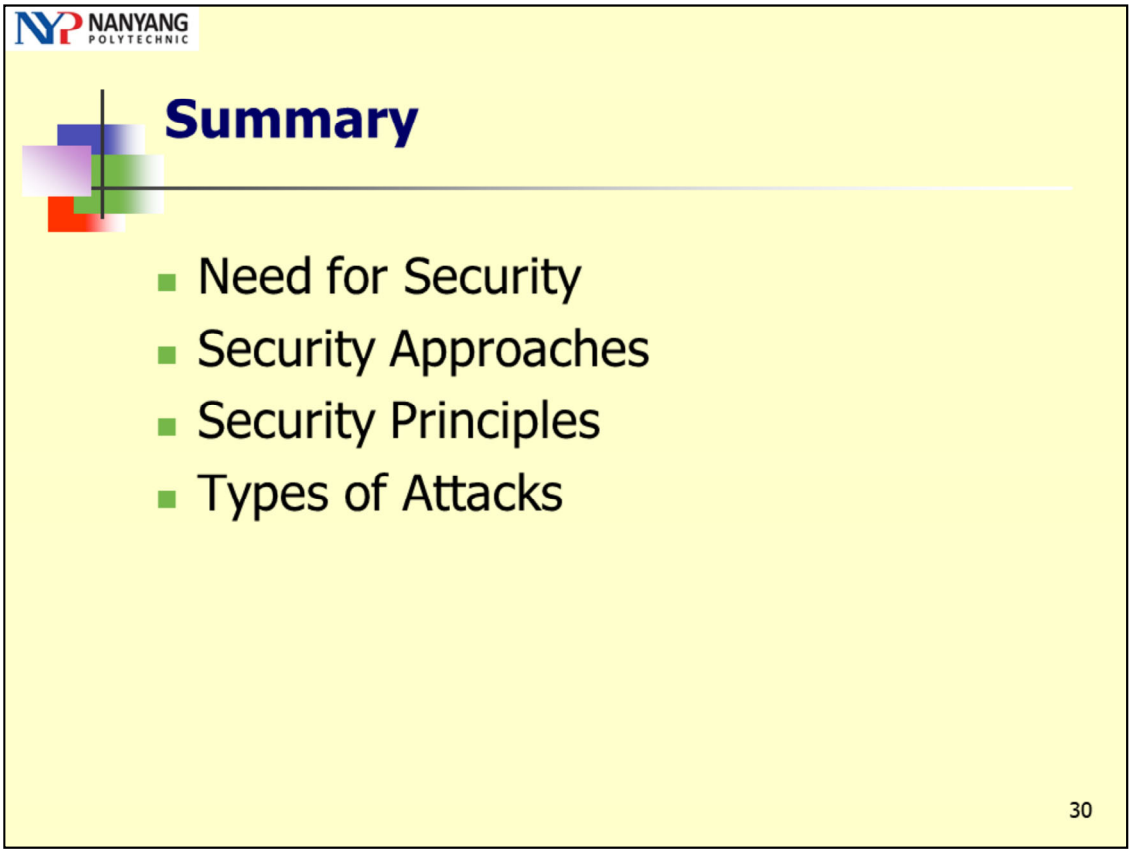


In a replay attack, the attacker captures and resends a message.

For example, an attacker can gain access to a resource

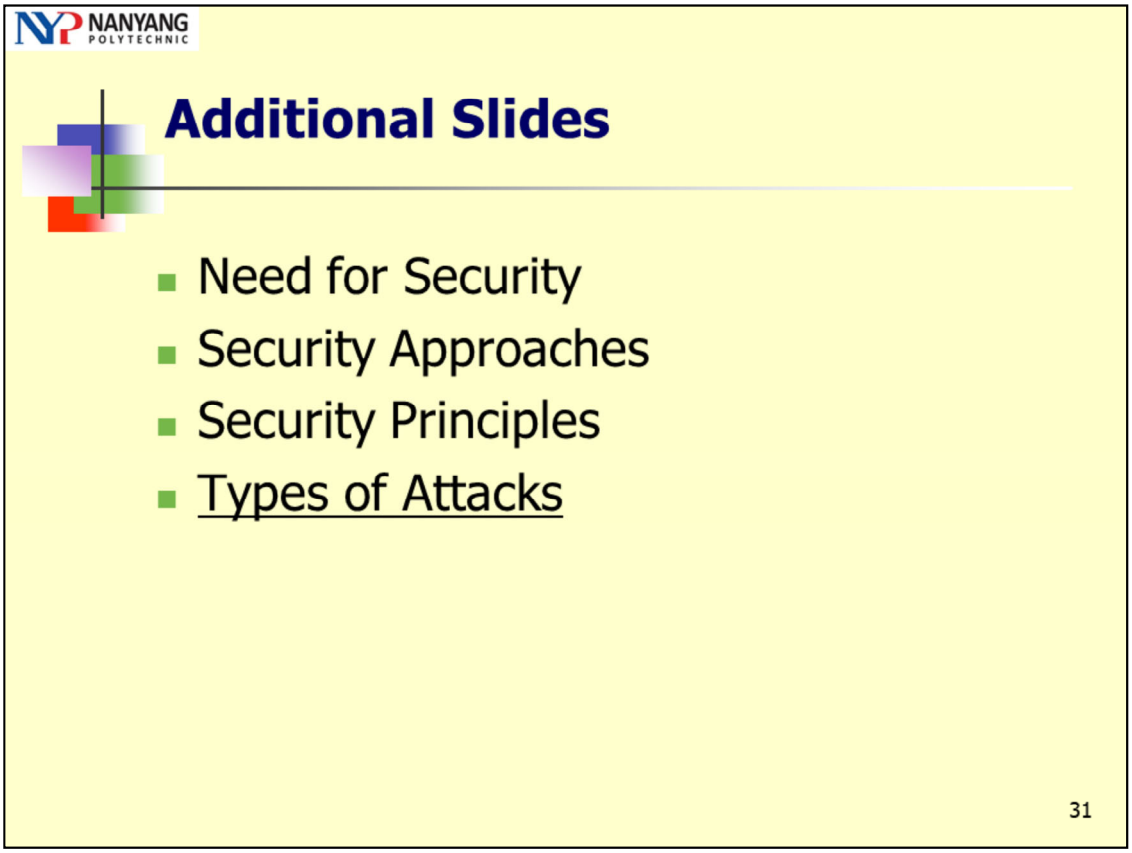
By resending authentication information to confuse the destination host.

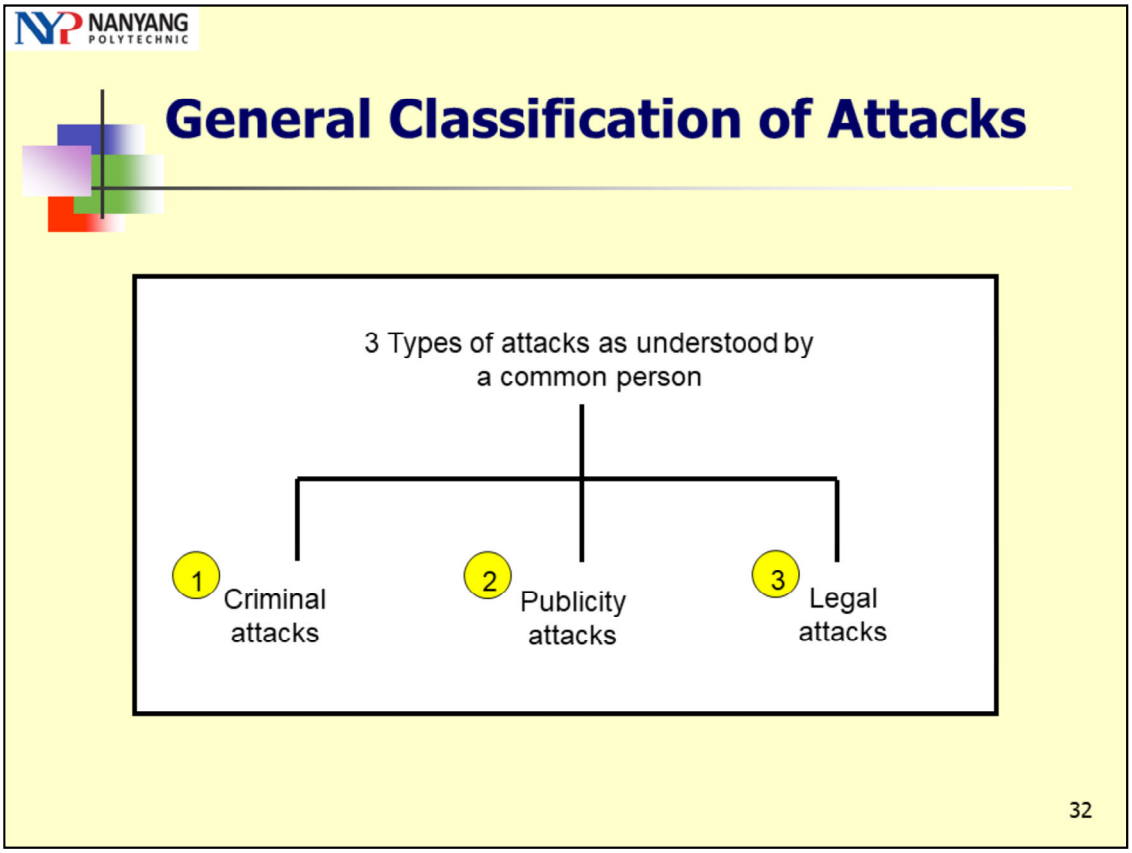
In alteration attack, the attacker captures and modifies the content of the original message.

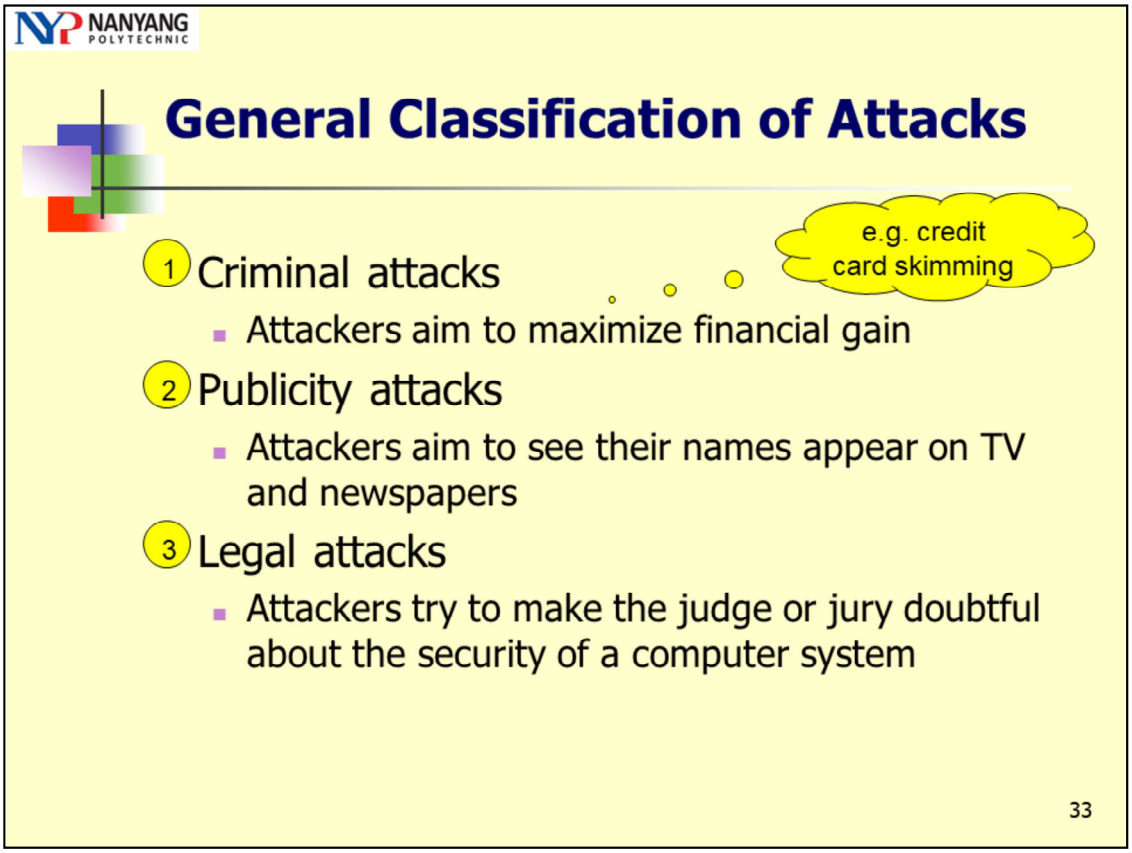


To recap, in this topic, we have learned how to:

- Describe the need for information security;
- Describe various security approaches;
- Describe some common security principles; and
- Describe some known types of computer attacks.

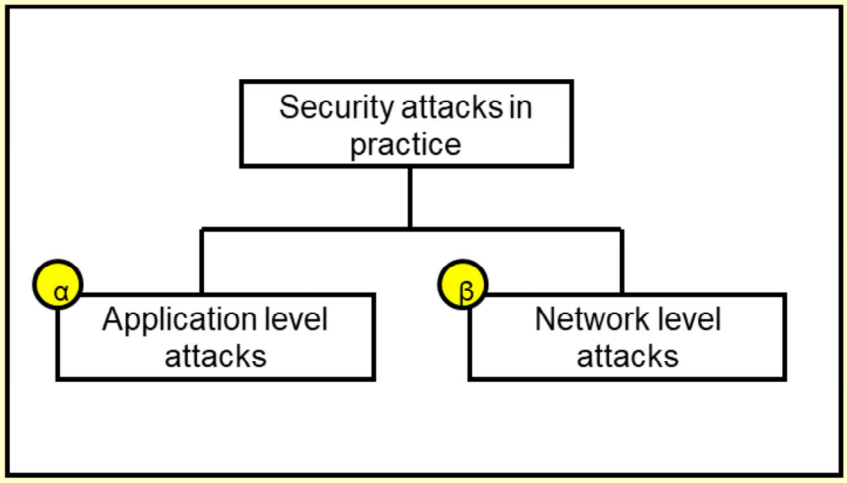

NANYANG POLYTECHNIC
Additional Slides
Need for Security
Security Approaches
Security Principles
Types of Attacks
31


NANYANG POLYTECHNIC
General Classification of Attacks
3 Types of attacks as understood by a common person
1
Criminal attacks
2
Publicity attacks
3
Legal attacks
32


NANYANG POLYTECHNIC
General Classification of Attacks
e.g. credit card skimming
1 Criminal attacks
Attackers aim to maximize financial gain
2 Publicity attacks
Attackers aim to see their names appear on TV and newspapers
3 Legal attacks
Attackers try to make the judge or jury doubtful about the security of a computer system
33

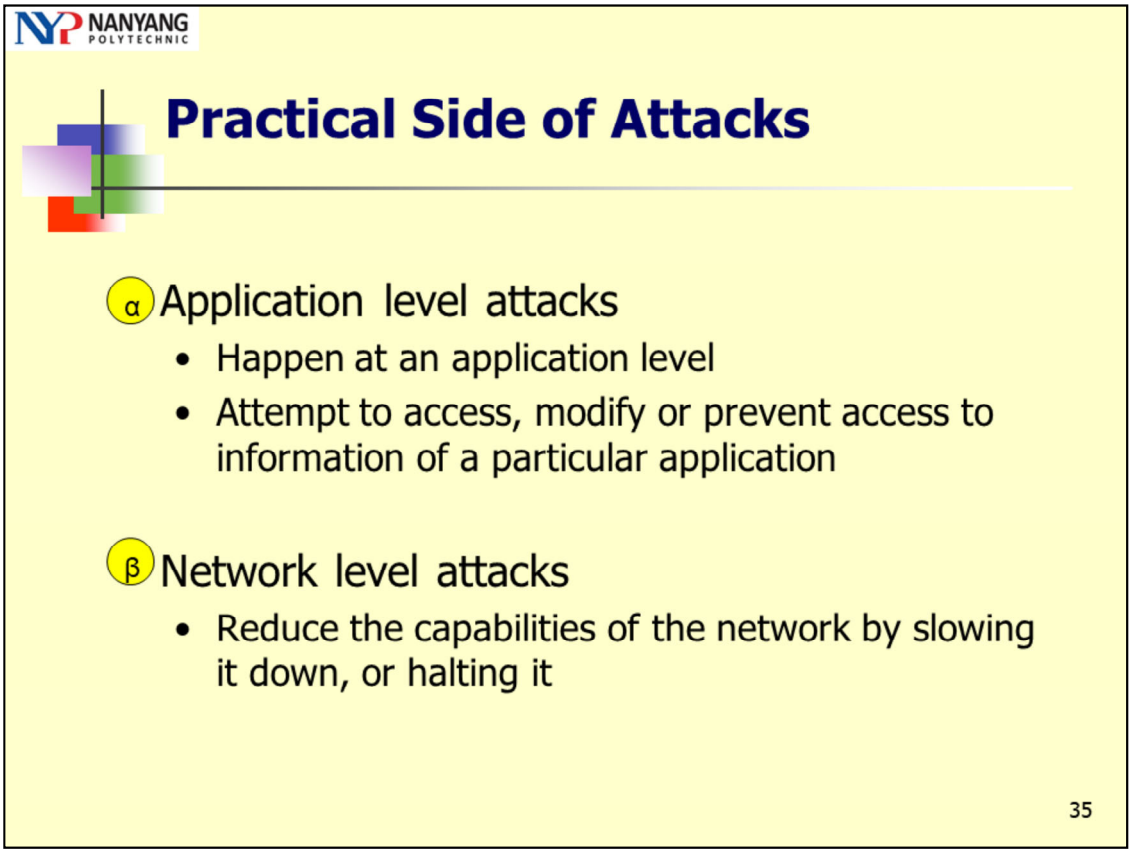
NANYANG POLYTECHNIC

Practical Side of Attacks



Attacks in real life are classified into application level attacks and network level attacks.

34


NANYANG POLYTECHNIC
Practical Side of Attacks
α Application level attacks
• Happen at an application level
• Attempt to access, modify or prevent access to information of a particular application
β Network level attacks
• Reduce the capabilities of the network by slowing it down, or halting it
35