什么是computer security
is defined as the protection (afforded) to (an automated)information system in order to attain the (applicable objectives of preserving) the integrity, availability, confidentiality of information system resources.
CIA : Confidentiality, Integrity, availability

C的原因：
need for keeping information secret arises from use of computers in sensitive fields
C的方法：
access mechanisms such as cryptography, support confidentiality
什么时候会损失C：
lost through unauthorized disclosure of information

I：often requires preventing unauthorized changes

分类：data integrity and origin integrity

方法：prevention mechanisms and detection mechanisms

包括 correctness 和 trustworthiness

什么时候会损失：lost through unauthorized modification or destruction of information

A:
attempts to block availability called denial of service attacks(DoS) are difficult to detect.

方法：ensures timely and reliable access of information

什么时候会损失：
lost through disruption of access to information (or information system).

区分：

authenticity : being genuine and able to be verified （or trust）; verifying that user are those who they say they are
accountability: actions of an entity can be traced uniquely to that entity;

三种security breach带来的影响程度：low, moderate, high

low: loss has limited adverse effect （minor, noticeably)
moderate : loss may serious adverse effect(significant)
high: severe or catastrophic adverse effect(major, severe)

Why do we need security ?
increased reliance on information technology
to safeguard the CIA of data transmitted over insecure networks.
Internet is not the only network in this world
many internal networks in organizations are prone to insider attacks

OSI security architecture:
IUT-T recommendation X.800 security architecture for OSI, which defines a systematic approach to assessing and providing security

The OSI security architecture focuses on security attacks, mechanisms and services.

什么是密码学?

（the study of mathematical） techniques related to （aspects of） information security such as confidentiality, integrity, entity authentication and data origin authentication.

confidentiality 的方法：physical protection, mathematical algorithms.

a safeguard is a countermeasure to protect against a threat.
a weakness in a safeguard is called a vulnerability.

什么是security attack : any action that compromises the security of information
什么是security mechanism: (a mechanism that is designed) to detect, prevent or recover from a security attack
什么是security service: a service that enhances the. security (of data processing systems and information transfers). A security service makes use of one or more security mechanisms.

threat : a potential for violation of security
attack : an assault on system security

attacks 分类：了解那几张图
interruption : attack on availability
interception: attack on confidentiality
modification: attack on integrity
Fabrication : attack on authenticity

threats 分类：了解那几个例子
disclosure, deception, disruption, usurpation

attacks还分类为passive and active
passive : attempt to learn or make use of information form the system, but does not affect system resources.
active: attempt to alter system resources or affect their operation

security services implement security policies and are implemented by security mechanisms

X.800 defines a security service as a service provided by the protocol layer of a communication system, that ensures adequate security of the systems or data transfers.

two types of program threats :
information access threats and service threats.