Security - Chapter 1- part 1

[1] How do we protect our most valuable assets? ازاي بنحمي الحاجات الغالية
Place them in a safe place like a bank ،حطهم في مكان أمان زي البنك

[2] Protecting assets was difficult. Today, protecting assets is easier. **WHY?**
زمان كانت الحماية صعبة دلوقت سهلة . ليييه؟

- **sophisticated alarm** and camera systems silently protect secure places like banks whether people are around or not.
  انذار متخصص زي كاميرا تراقب الاماكن بهدوء سواء فيه ناس أو لأ
- The techniques of **criminal investigation** have become so effective that a person can be identified by genetic material (DNA), fingerprints, retinal patterns, voice
  وسائل التحقيق الجنائي تقدر تتعرف على شخص بالدي ان ايه أو بالبصمة أو الصوت
- The assets are **stored in a safer form**. For instance, many banks now contain less cash because much of a bank's business is conducted with checks, electronic transfers, credit cards, or debit cards.
  الحاجات بتتخزن في أماكن آمنة، مثلا البنوك مافيهاش كاشات كتير وبيتعاملو بالشيكات والكريدت
- improvements in **transportation and communication** mean that police can be at the scene of a crime in minutes;
  وسائل النقل والاتصالات بتخلي البوليس في مسرح الجريمة في مينيت (دقايق)
- From the **criminal's point of view, the risk** is so high that there are easier ways than bank robbery to make money.
  من وجهة نظر عمو المجرم ، الخطر عالي ، وبالتالي الشغل أسهل من سرقة البنك

[3] What Does "Secure" Mean? طب يعني ايه أمن؟

- "**security system**" protects our house, warning the neighbors or the police if an unauthorized intruder tries to get in.

- children's "**physical security**," hoping they are safe from potential harm.
- "**computer security**": we mean that we are addressing three important aspects of any computer-related system: **confidentiality**, **integrity,** and **availability.**

➔[4] What is Computer Security? ده تعريف أمن الحاسب

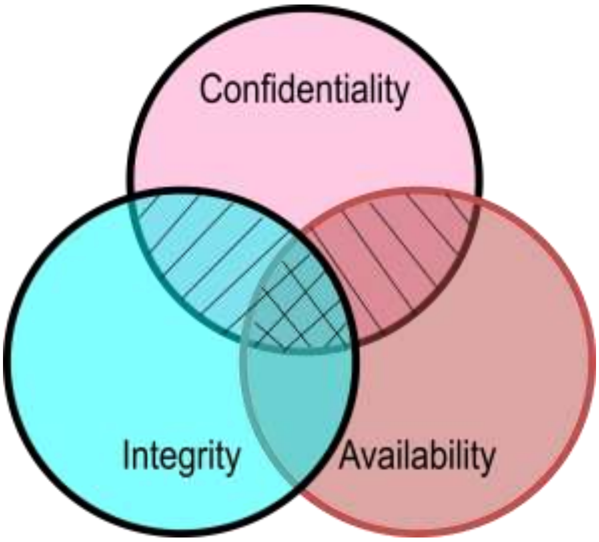
The **protection** afforded to an automated **information system**
to attain the objectives of preserving the **integrity, availability & confidentiality**
حماية أنظمة المعلومات لتحقيق التكامل والاتاحة والسرية
of information system resources (includes **hardware, software, information/data**, and telecommunications) لكل حاجة : الهاردوير والسوفتوير والبيانات وأجهزة الاتصالات والمحشي

➔[5] Security Goals

- **Confidentiality** ensures that computer-related assets are accessed only by authorized parties. That is, only those who should have access to something will actually get that access. By "access," we mean not only reading but also viewing, printing, or simply knowing that a particular asset exists. Confidentiality is sometimes called **secrecy** or **privacy**.

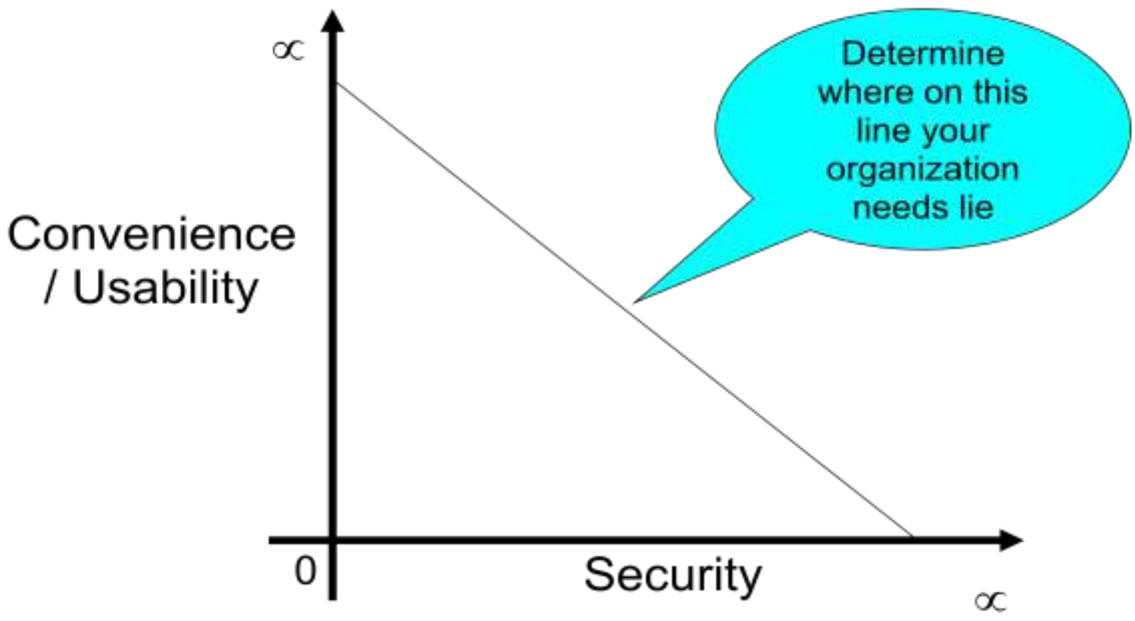
- **Integrity** means that assets can be modified only by authorized parties or only in authorized ways. In this context, modification includes writing, changing, changing status, deleting, and creating.

- **Availability** means that assets are accessible to authorized parties at appropriate times. In other words, if some person or system has legitimate access to a set of objects, that access should not be prevented. For this reason, availability is sometimes known by its opposite, denial of service.



challenges in building a secure system is finding the right balance among the goals, which often conflict. For example, it is easy to preserve a particular object's confidentiality in a secure system simply by preventing everyone from reading that object. However, this system is not secure, because it does not meet the requirement of availability for proper access. That is, there must be a balance between confidentiality and availability.

But balance is not all. In fact, these three characteristics can be **independent**, can overlap, and can even be **mutually exclusive**. For example, we have seen that strong protection of confidentiality can severely restrict availability.



➔Confidentiality

You may find the notion of confidentiality to be straightforward: **Only authorized people or systems can access protected data.** However, as we see in later chapters, ensuring confidentiality can be difficult.

By "accessing" data, do we mean that an authorized party can access a single bit? the whole collection? pieces of data out of context? Can someone who is authorized disclose those data to other parties?

Confidentiality is the security property we understand best because its meaning is narrower than the other two. We also understand confidentiality well because we can relate computing examples to those of preserving confidentiality in the real world.

➔ Integrity

integrity means different things in different contexts. When we survey the way some people use the term, we find several different meanings. For example, if we say that we have preserved the integrity of an item, we may mean that the item is

- **Precise =accurate= دقيقة**
- **Unmodified = لا تعدل**
- **modified only in acceptable ways تعدل بطرق مسموح بيها**
- **modified only by authorized people تعدل بناس مسموح ليها**
- **modified only by authorized processes تعدل بعمليات مسموح بيها**
- **consistent, internally consistent مظبوطة برة وجوة**
- **meaningful and usable لها معنى**

Integrity can also mean two or more of these properties.
It recognizes **three aspects** of

integrity authorized **actions**
separation and **protection** of resources,
and **error** detection and correction.

Integrity can be **enforced** in much the same way as can confidentiality:

by control of **who** can access **which** resources in **what ways**.

Some forms of integrity are well represented in the real world, and those precise representations can be implemented in a computerized environment. But not all interpretations of integrity are well reflected by computer implementations.

➔Availability

Availability applies both to data and to services (that is, to information and to information processing), and it is similarly complex.
Meaning of availability: an object or service is thought to be available if

- It is present in a **usable** form.
- It has **capacity** enough to meet the service's needs.
- It is making **clear progress**, and, if in wait mode, it has limited waiting time.
- The service is **completed** in an acceptable period of time.

We can construct an overall description of availability by combining these goals. We say a data item, service, or system is available if

- There is a **timely response** to our request.
- **Resources are allocated fairly** so that some requesters are not favored over others.
- The service or system involved follows a philosophy of **fault tolerance**, whereby hardware or software faults lead to graceful cessation of service or to work-arounds rather than to crashes and abrupt loss of information.
- The service or **system can be used easily** and in the way it was intended to be used.
- **Concurrency** is controlled; that is, simultaneous access, deadlock management, and exclusive access are supported as required.

Much of computer security's past success has focused on confidentiality and integrity; full implementation of availability is security's next great challenge.