LECTURER

DR.

MOHAMMED

NASSER

AL-KHWLANI

CYBER SECURITY PROGRAM

INTRODUCTION TO INFORMATION SECURITY

COMMUNICATION BY

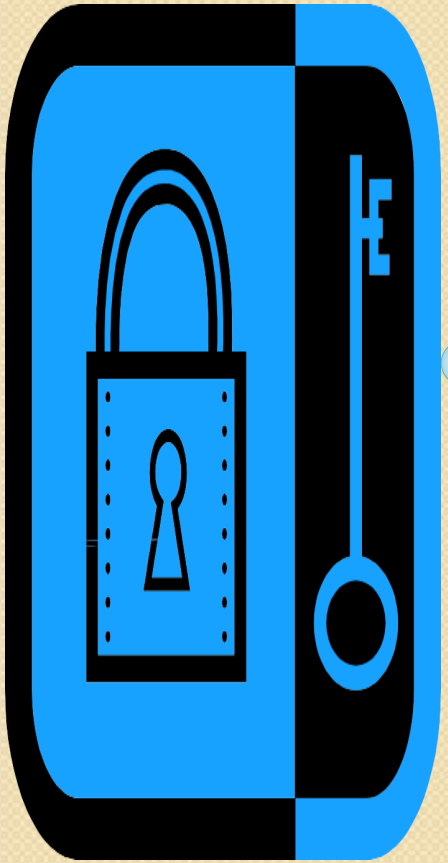
TEL/WATSUP

777040098

EMAIL:

MNASER201435@GMAI.COM

COURSE OUTLINE



1 INTRODUCTION

2- VULNERABILITIES

3- TYPES OF ATTACKS AND CONTROL

4-AUTHENTICATION

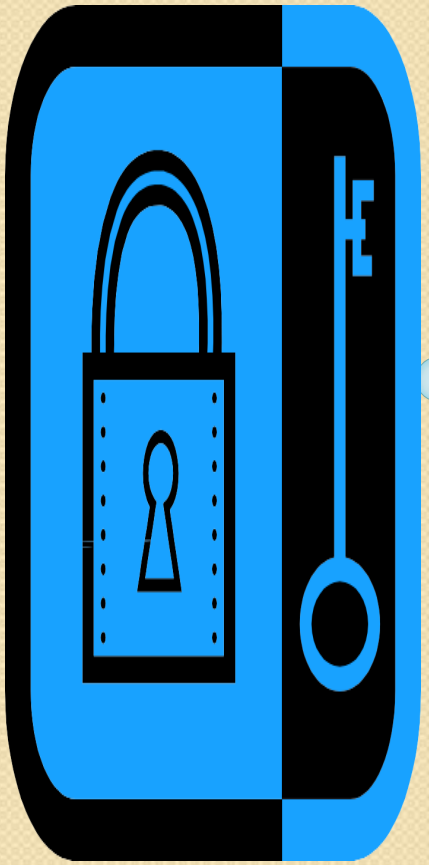
5-ACCESSES CONTROLS

6- SECURITY POLICIES

8,9,10 ENCRYPTION

11,12 DATABASE SECURITY

Assements Methods



10% Attendance

10% Participants

20% Mid Exam

60% Final Exam

Lecture 1:

Introduction to

Information Security

What Does "Secure" Mean?
ماذا يعني مأمون

- How do we protect our most valuable assets?

كيف نحمي ممتلكاتنا ذات الأكثر قيمة؟

- ✓ One option is to place them in a safe place,
  - like a bank.
  - أحد الخيارات هو وضعهم في مكان أمن مثل البنك

Overview (نظرة عامة)

- ***Early***, the bank robberies are more;
  - ✓Kept large amount of cash, gold & silver, which could not be traced easily,
  - ✓ من وقت مبكر أكثر الأشياء التي تتعرض للسرقات من البنوك هي النقود ، الذهب، الفضة و التي من الصعب تتبع أثرها عند سرقتها.
  - ✓Communication & transportation facilities it might be;
  - ✓سهولة الاتصال و النقل ربما تكون ساعات قبل ابلاغ المسؤولين بالسرقة
    - — hours before the legal authorities were informed of a robbery, and
    - — days before they could actually arrives at the scene of the crime. (أيام قبل أن يصلوا فعليا إلى مكان الجريمة)
  - ✓A single guard for the night was only marginally effective, (مناوب واحد في الليل يكون تأثيره هامشي)

Overview

- ***Today***; many factors work against the potential criminal; (اليوم عوامل عديدة تعمل ضد المجرم المحتمل)

  Very sophisticated (متطورة جدا)

  - ✓ **alarm systems** (أنظمة المر اقبة)
  - ✓ **camera systems** (أنظمة كاميرات المر اقبة)
  - ✓ **silently protect secure places;** (أمكان حماية سرية مثل البنوك)
    - ➢ **Ex.; banks.**

- The techniques of criminal investigation have become very effective; (طرق البحث عن المجرمين أصبحت فعالة جدا)

  ☞ **a person can be identified by;**(يمكن تمييز الشخص ب)

  – **Fingerprint**(البصمة) **, voice recognition**(تمييز الصوت)**, composite sketch**(الرسوم التخطيطية المركبة من مسرح الجريمة)**, ballistics evidence** (الأدلة البلاستكية)**,**

  – **retinal patterns** (شبكة العين)**, and**

  – **genetic material (DNA).** (الحمض النووي) المواد الجينية

Overview (3)

- Much of a bank's business is conducted with;
- أكثر أعمال البنوك تدار ب
  - ✓ **Checks (الشيكات) ,**
  - ✓ **electronic transfers (التحويل الالكتروني),**
  - ✓ **credit cards, or (بطائق الإئتمان الالكترونية)**
  - ✓ **debit cards**. (بطائق الدين)
- Sites that do stores *large amounts* of cash or currency are protected with many levels security:

أماكن خزن الكميات الضخمة من النقود و العملات يتم حمايتها بعدة مستويات

- ✓ **Several layers of physical systems (أنظمة فيزيائية ذو طبقات متعددة),**
- ✓ **complex locks(أقفال معقدة) ,**
- ✓ **multiple-party systems requiring the agreement of several people to allow access.**

(أنظمة تتطلب مو افقة عدة أشخاص للسماح بالوصول)

خصائص التدخل في الحاسوب
Characteristics of Computer Intrusion

- Any part of a computing system can be the target of a crime;
  أي جزء في نظام الحوسبة يمكن أن يكون هدفا للجريمة
- **A *computing system* is a collection of:**

  نظام الحوسبة هو مجموعة من المكونات التالية

  ✓ HW, SW, (جزء مادي و جزء برمجي)

  ✓ storage media, data, and (وسائط خزن و بيانات)

  ✓ persons that an organization uses to do computing **tasks**.

  أشخاص من يستخدمون النظام لإنجاز المهام
- **The obvious target of a bank robbery is each;**

  الهدف الواضح لسرقة البنك هي ما يلي

  ✓ A list of names & addresses of depositors, (قائمة أسماء و عناوين المودعين)

  ✓ A list might be: وهذه القائمة يمكن أن تكون

  — On paper, Recorded on a magnetic medium,(على ورقة أو مخزنة الكترونيا)

  — Stored in internal computer memory, orمخزنة في ذاكرة داخلية للحاسوب

  — transmitted over telephone lines, or satellite links.

  — منقولة على خطوط التليفون أو على الأقمار الصناعية

Characteristics of Computer Intrusion

- A **competing bank** can use this information to:

بنك منافس يمكن أن يستخدم معلومات المودعين لعمل ما يلي:

- ✓ steal clients or even to disrupt service,

سرقة العملاء أو حتى تعطيل الخدمة

- ✓ Discredit the bank, (تشويه سمعة البنك)
- ✓ An unscrupulous individual could ***move money*** from one ***account*** to another without the owner's permission,

شخص عديم الضمير يمكن أن يحول نقودا من حساب إلى اخر من دون إذن صاحبه

- ✓ A group of con artists could contact large depositors and convince them to invest in fraudulent schemes.

مجموعة من محترفي التضليل يمكن أن يتواصلون مع مودعين كبار و إقناعهم بالاستثمار في مخططات التضليل أو الخداع.

Characteristics of Computer Intrusion (3)

- Example:

✓A robber intent on *stealing something from a house* will *not attempt to penetrate a two-inch-thick metal door* if a window gives easier access.

سارق ينوي سرقة بعض الأشياء من منزل لن يحاول أن يتسلل من الباب الثخين إذا كانت النافذة تعطي وصولا أسهل

- The weakest point is the most serious vulnerability;

النقطة الأكثر ضعفا هي الأكثر خطورة للاختراق

- **A *Principle of Easiest Penetration*:** مفهوم الاختراق الأسهل

'An intruder must be expected to use any available means of penetration'

"المخترق يجب أن يكون متوقعا منه استخدام الأدوات **المتاحة** للاختراق أو الهجوم "

What Is Computer Security?
ما هي أمنية الحاسوب

- **Computer security** is the protection of the items that have value, called the assets of a computer or computer system;

أمنية الحاسوب هي حماية المكونات أو الأجزاء الأكثر قيمة و التي تسمى أصول الحاسوب أو نظام الحاسوب.

- ✓ There are many types of assets, involving;

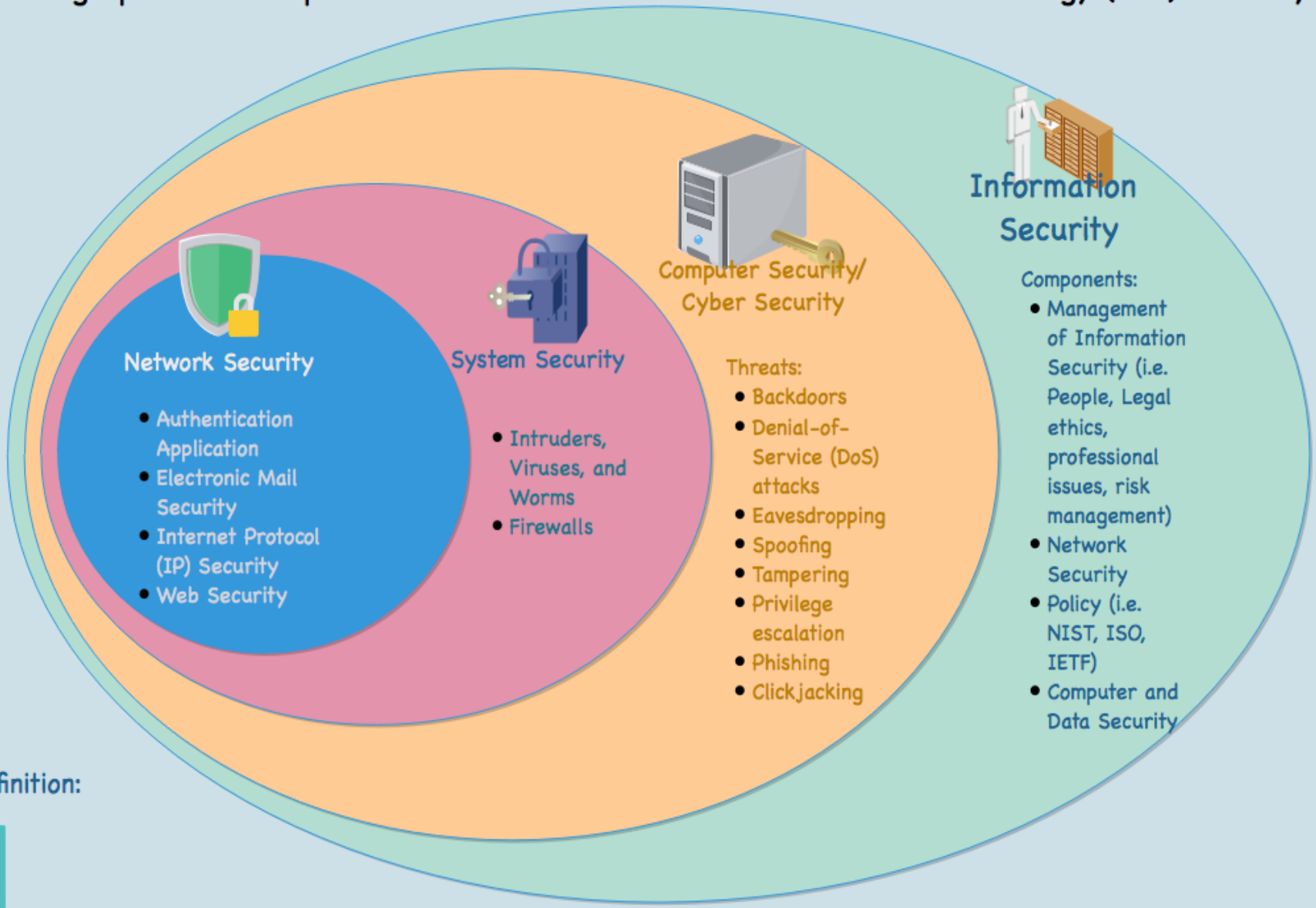
تتضمن الأصول عدة أنواع منها:

  - ☞ HW, SW, data, people, processes, or combinations of these.

المعدات المادية و البرمجيات و الأشخاص و العمليات او الربط بينها جميعا

- ✓ To determine what to protect; **لتحديد ما يتم حمايته**
  - ☞ we must first identify يجب أولا أن نحدد الأصل المراد حمايته
  - ☞ what has value and to whom. ما الذي له قيمة و من يملكه

Infographics on Components of Information and Communications Technology (ICT) Security



by definition:

- Communications security – to protect communications media, technology, and content.
- Network security – to protect networking components, connections, and contents.
- Information security – to protect information assets.

- aziyati, apr 2017

Computer Objects of Value

Hardware:

- Computer
- Devices (disk drives, memory, printer)
- Network gear

Software:

- Operating system
- Utilities (antivirus)
- Commercial applications (word processing, photo editing)
- Individual applications

Data:

- Documents
- Photos
- Music, videos
- Email
- Class projects

Values of Assets; (قيم الممتلكات)

- After identifying the assets to protect, we next determine their value; (بعد تحديد الممتلك لحمايته يتم بعدها تحديد قيمته)
- The value of an asset depends on; (قيمة الممتلك تعتمد على)
  - ✓ the asset owner's or user's perspective, and وجه نظر المالك
  - ✓ it may be independent of monetary cost,

    (ربما تكون القيمة مستقلة عن الكلفة النقدية)

Values of Assets

Off the shelf; easily replaceable

Hardware:
- Computer
- Devices (disk drives, memory, printer)
- Network gear

Software:
- Operating system
- Utilities (antivirus)
- Commercial applications (word processing, photo editing)

Data:
- Documents
- Photos
- Music, videos
- Email
- Class projects

- Individual applications

Unique; irreplaceable

Definition of Information Security
تعريف أمنية المعلومات

- **Information Security**;
  - ✓ is the protection of information and its critical elements, including the systems and HW that use, store, and transmit that information,
  - ✓ أمنية المعلومات هي حماية المعلومات و عناصرها الحرجة و التي تشمل النظام و المعدات المادية التي تستخدم لخزن و نقل المعلومات.
  - ✓ information security includes the broad areas of information security management, computer & data security, and network security, and Cyber Security.
  - ✓ تشمل أمنية المعلومات مجالات واسعة مثل إدارة أمنية المعلومات ،أمنية البيانات أمنية الشبكات، و الأمن السيبراني.

Computer security Goals (أهداف أمنية الحاسوب)

- A Computer security means that we are addressing three important properties/goals of any computer-related system;
  - أمنية الحاسوب تعني أننا نحدد ثلاث خصائص أو أهداف لأي نظام حاسوبي

1-Confidentiality: the ability of a system to ensure that an asset is viewed only by authorized parties,

الموثوقية و تعني قدرة النظام على التأكيد أن الممتلكات تعرض فقط لمن يسمح لهم

– means that the assets of computing system are accessible only by authorized parties,

و تعني الموثوقية أن أجزاء نظام الحوسبة قابلة للوصول من قبل الأطراف المسموح لها

☞ "read"-type access: reading, viewing, printing.

Computer Security Goals

*2-**integrity***: the ability of a system to ensure that an asset is modified only by authorized parties,

التكاملية و تعني قدرة النظام على التأكيد أن البيانات تعدل من قبل المخولين بذلك فقط.

- means that assets can be modified by authorized parties,
  - ☞ writing, changing status, deleting, and creating

*3-**Availability***: the ability of a system to ensure that an asset can be used by any authorized parties,

التوفر و يعني قدرة النظام على التأكيد أن أي جزء يمكن استخدامه من قبل أي شخص مسموح به في الأوقات المناسبة.

- means that assets are accessible to authorized parties at appropriate times, (*denial of service*).

Balance of The Security Goals