Borg El Arab Technological University

جامعة برج العرب التكنولوجية
BORG AL ARAB TECHNOLOGICAL UNIVERSITY

Introduction to Cyber Security
مقدمة الأمن السيبراني

1st Level – 1st Semester

د/ أشرف عبدالعزيز طه

Course Content in Lectures

- Chapter 1 - Introduction المقدمه
- Chapter 2 - Classical Encryption/Decryption Techniques

تقنيات التشفير/فك التشفير التقليدية

- Chapter 3 - Modern Encryption/Decryption Techniques

تقنيات التشفير/فك التشفير الحديثة

- Chapter 4 - Attacks and Prevention Techniques

الهجمات وتقنيات الوقاية منها

- Chapter 5 - Virus and Antivirus الفيروسات ومكافحة الفيروسات
- Chapter 6 - Ethical Hacking القرصنة الأخلاقية

Agenda

- Chapter 1 **Introduction**
  - Cyber Security الأمن السيبراني
  - Categories of Cyber Security فئات الأمن السيبراني
  - Importance of Cyber Security أهمية الأمن السيبراني
  - Types of Cyber Threats أنواع التهديدات السيبرانية
  - Expected outputs after teaching this course

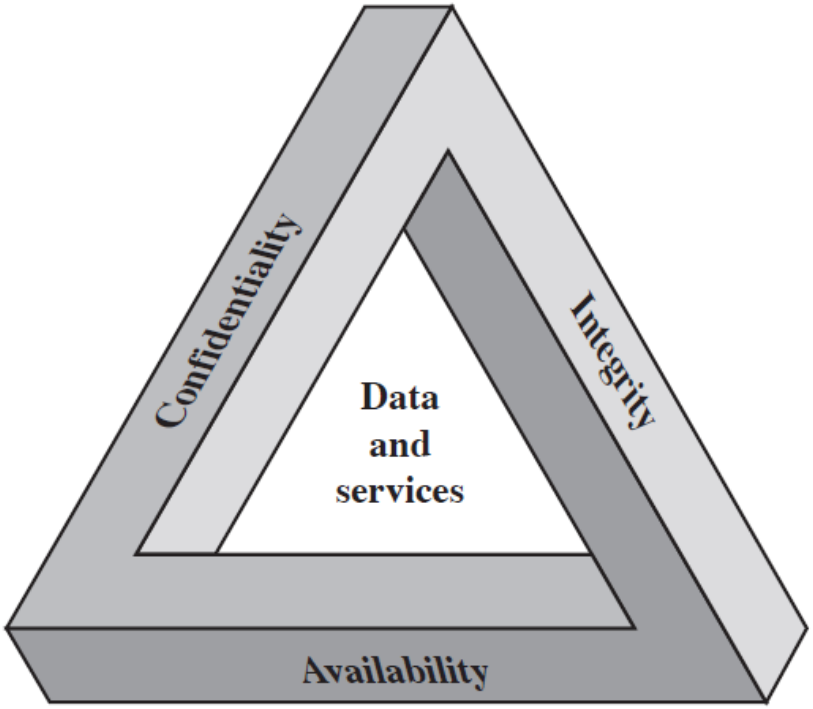
    المخرجات المتوقعة بعد تدريس هذا المقرر

Introduction to Security

- **Definition of Computer Security**

  The protection provided to a system in order to attain the integrity, availability, and confidentiality of information system resources

الحماية المقدمه للنظام للحصول على سلامة وتوفير وسرية موارد نظام المعلومات.



Confidentiality	**السرية**
Integrity	**السلامه والحماية**
Availability	**توافر**
Data and Services	**البيانات والخدمات**

- **Confidentiality**
  - **Data confidentiality**: confidential information is not made available to unauthorized persons.

    المعلومات السرية لا تكون متاحه للأشخاص غير الموثقين.
  - **Privacy**: Users control what information related to them may be collected and stored.

    يتحكم المستخدمون في المعلومات المتعلقة بهم التي يتم جمعها وتخزينها
- **Integrity**
  - **Data integrity**: information and programs are changed only in a specified and authorized manner

    يتم تغيير المعلومات والبرامج فقط بطريقة محددة ومصرح بها
  - **System integrity**: system performs its intended function free from unauthorized manipulation

    يؤدي النظام وظيفته المقصودة دون تلاعب غير مصرح به
- **Availability**
  - Systems work on time and service is provided to authorized users

    تعمل الأنظمة في الوقت المحدد ويتم توفير الخدمة للمستخدمين المصرح لهم

- **Security attack**:

Any action that caused dangerous to the security of information.

أي إجراء يسبب خطورة على أمن المعلومات

- **Security mechanism**:

A process designed to detect, prevent, or recover from a security attack.

عملية مصممة للكشف عن هجوم أمني أو منعه أو التخلص منه

- **Security service**: A processing or communication service that enhanced the security of the data processing systems and the information transfers of an organization.

خدمة معالجة أو اتصال تحسن أمن أنظمة معالجة البيانات ونقل المعلومات للمؤسسة.

• Note terms

- **Threat**: a potential for violation of system security.

ثغره يتم منها هجوم على أمن النظام

- **Attack**: an assault on system security

هجوم على أمن النظام

Security Attacks

- **Passive attacks**
  - Include unauthorized reading of a message and traffic analysis.

    يتضمن قراءة غير مصرح بها لرسالة وتحليل حركة المرور

- **Active attacks**
  - Modification of messages or files, and denial of service.

    تعديل الرسائل أو الملفات ورفض الخدمة

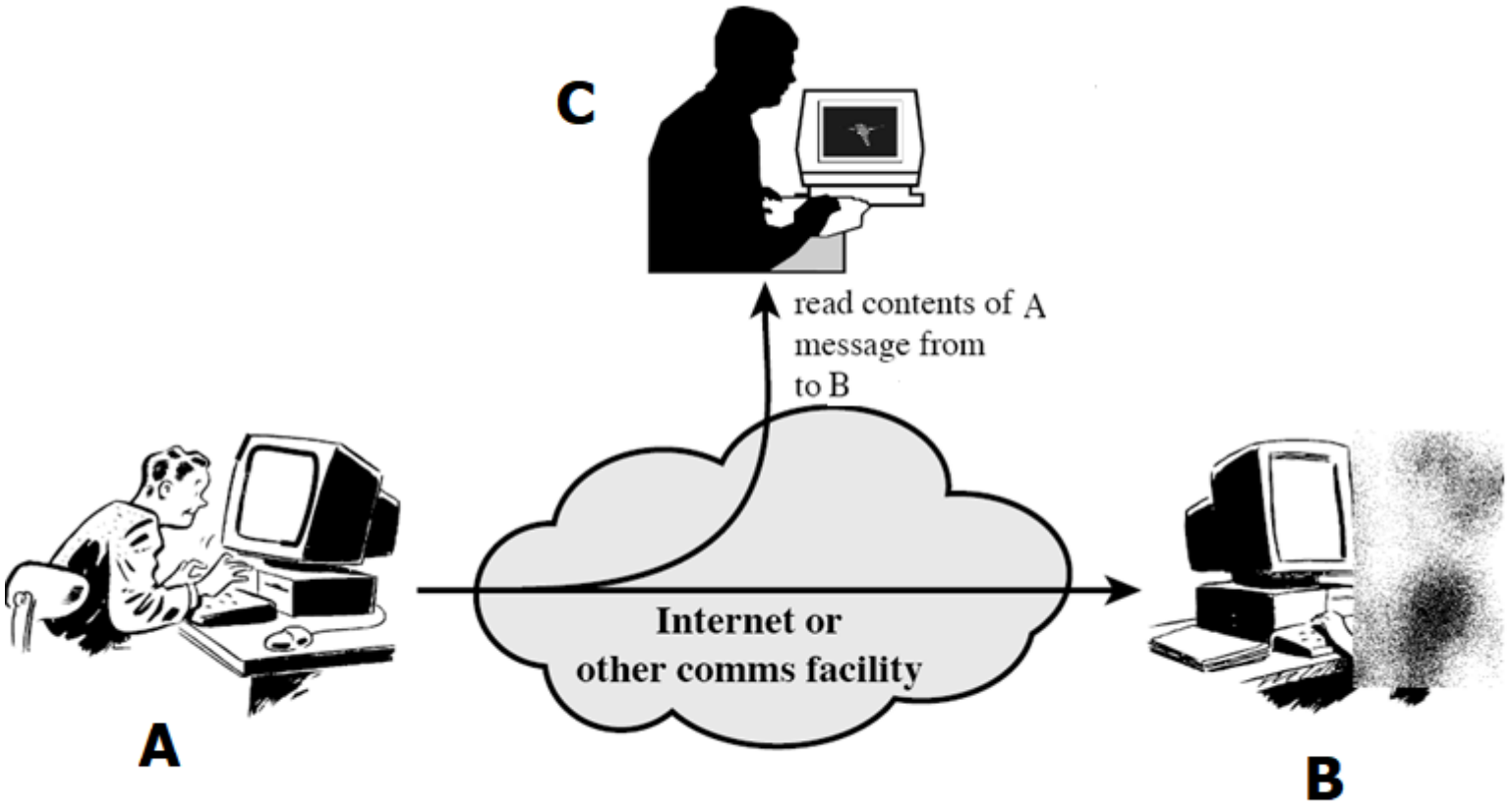
Passive Attacks

- Eavesdrop, monitor signal transmission التصنت أو مراقبة نقل الإشارة
- Obtain information being transmitted الحصول على المعلومات التي يتم إرسالها
- **Type 1:** Release of message contents معرفة محتويات الرسالة
  - tap on phone line to hear conversation التصنت على خط الهاتف لسماع المحادثة
  - get unauthorized copy of email message
    الحصول على نسخة غير مصرح بها من رسالة البريد الإلكتروني
- **Type 2:** Traffic analysis تحليل الإشارة
  - observe message pattern, even if encrypted مراقبة شكل الرسالة، حتى لو كانت مشفرة
  - determine location and identity of parties تحديد موقع الأطراف وهويتها

Very difficult to detect; no alteration of data

من الصعب جدا اكتشافها ؛ لا تغيير في البيانات

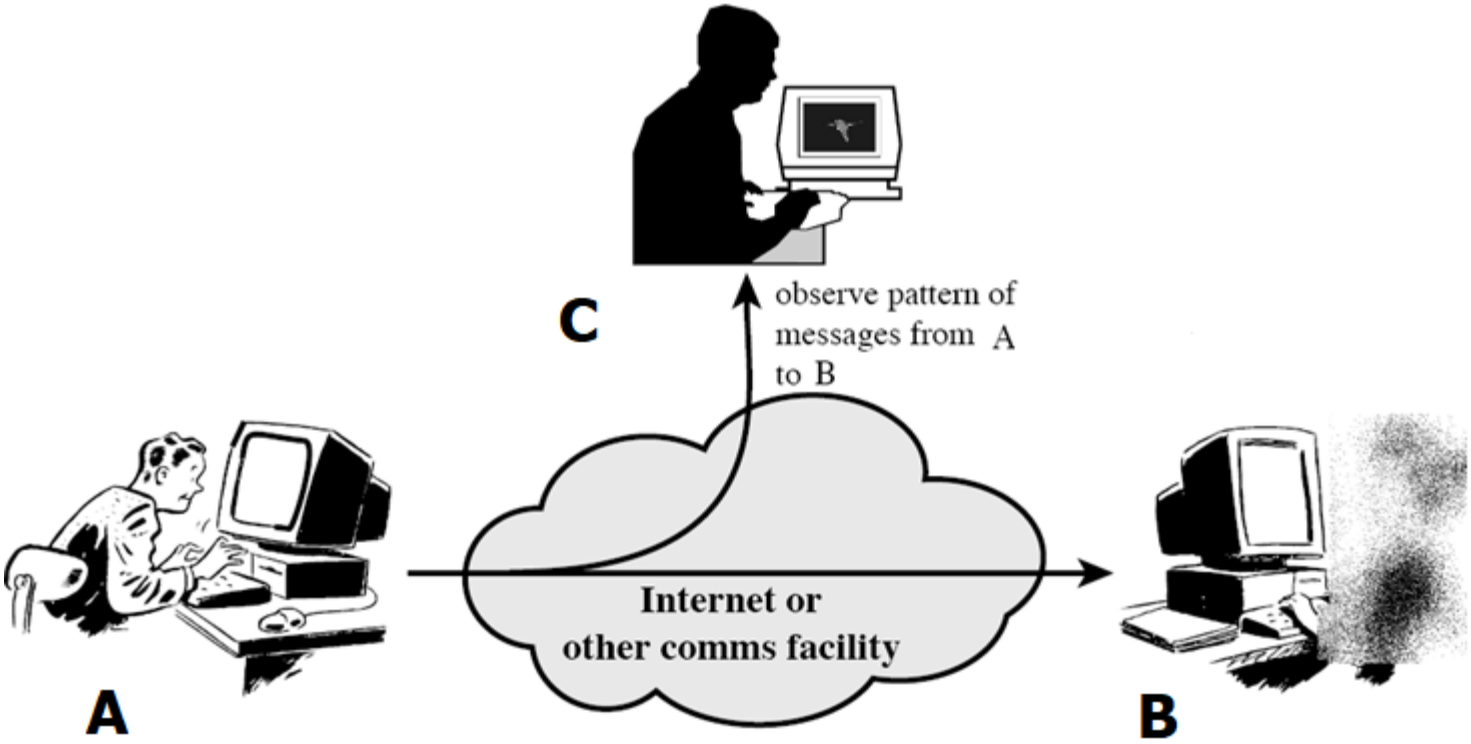
Passive Attacks



(a) Release of message contents

معرفة محتويات الرسالة

Passive Attacks



(b) Traffic analysis

تحليل الإشارة

Active Attacks

- Modification of transmitted data or creating false data

تعديل البيانات المرسلة أو إنشاء بيانات خاطئة

  - **Type 1:** Masquerade الإنتحال
    - pretend to be a different entity إنتحال شخص مختلف
  - **Type 2:** Replay إعادة
    - capture data for subsequent retransmission

التقاط البيانات لإعادة الإرسال مره أخرى

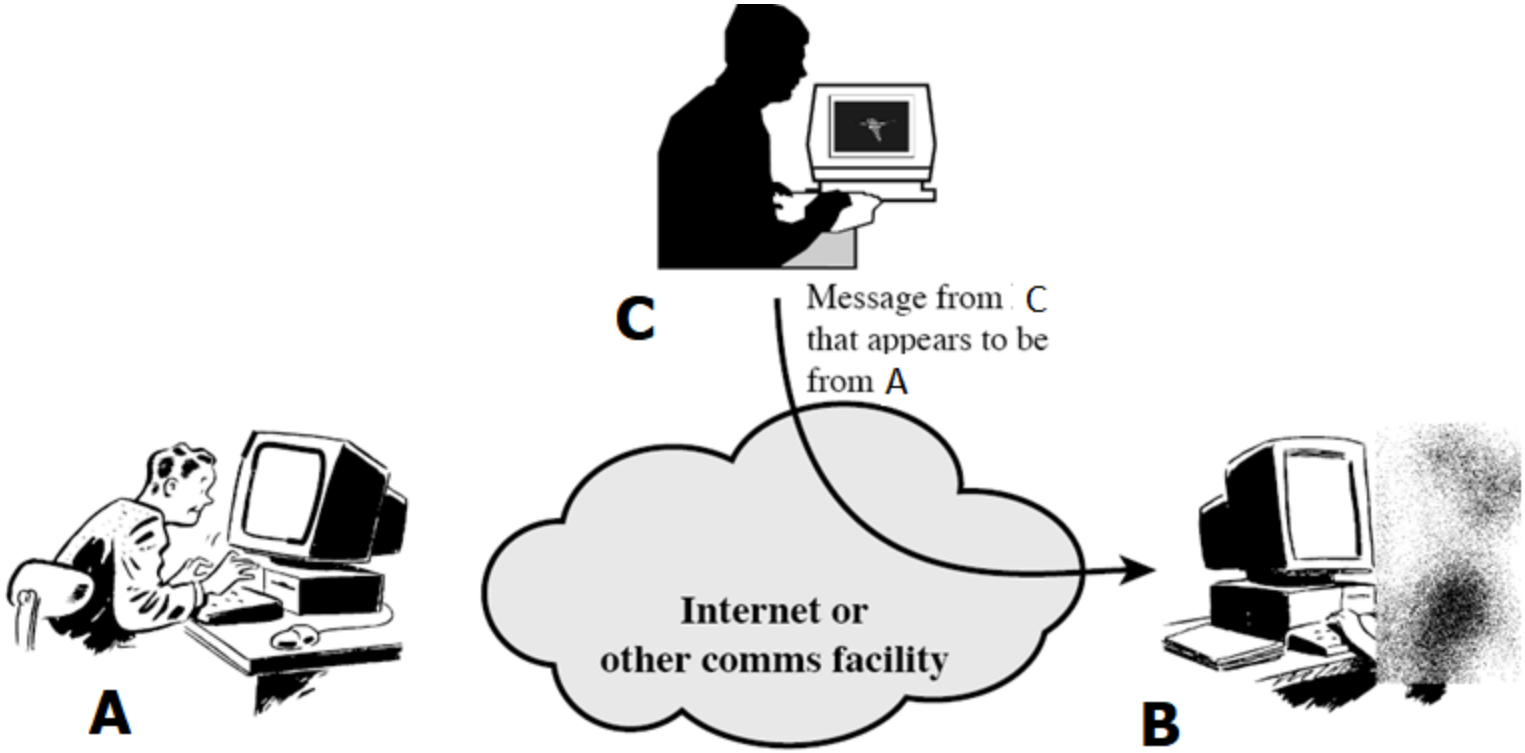
  - **Type 3:** Modification of message تعديل الرسالة
    - some portion of legitimate message is altered

يتم تغيير جزء من الرسالة الموثقة

  - **Type 4:** Denial of service الحرمان من الخدمة
    - disruption of network by disabling or overloading

تعطيل الشبكة عن طريق التعطيل أو التحميل الزائد

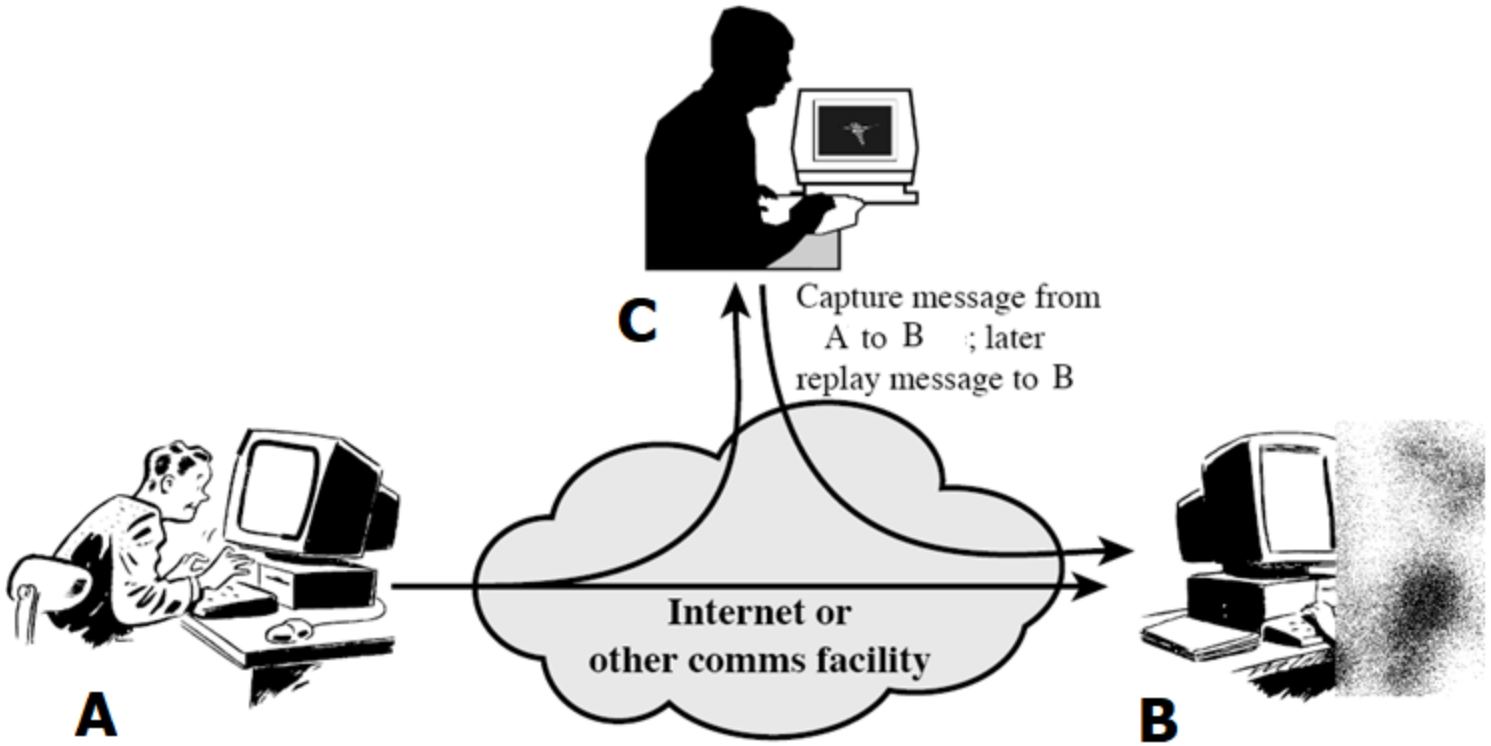
Active Attacks



(a) Masquerade

إنتحال شخص مختلف

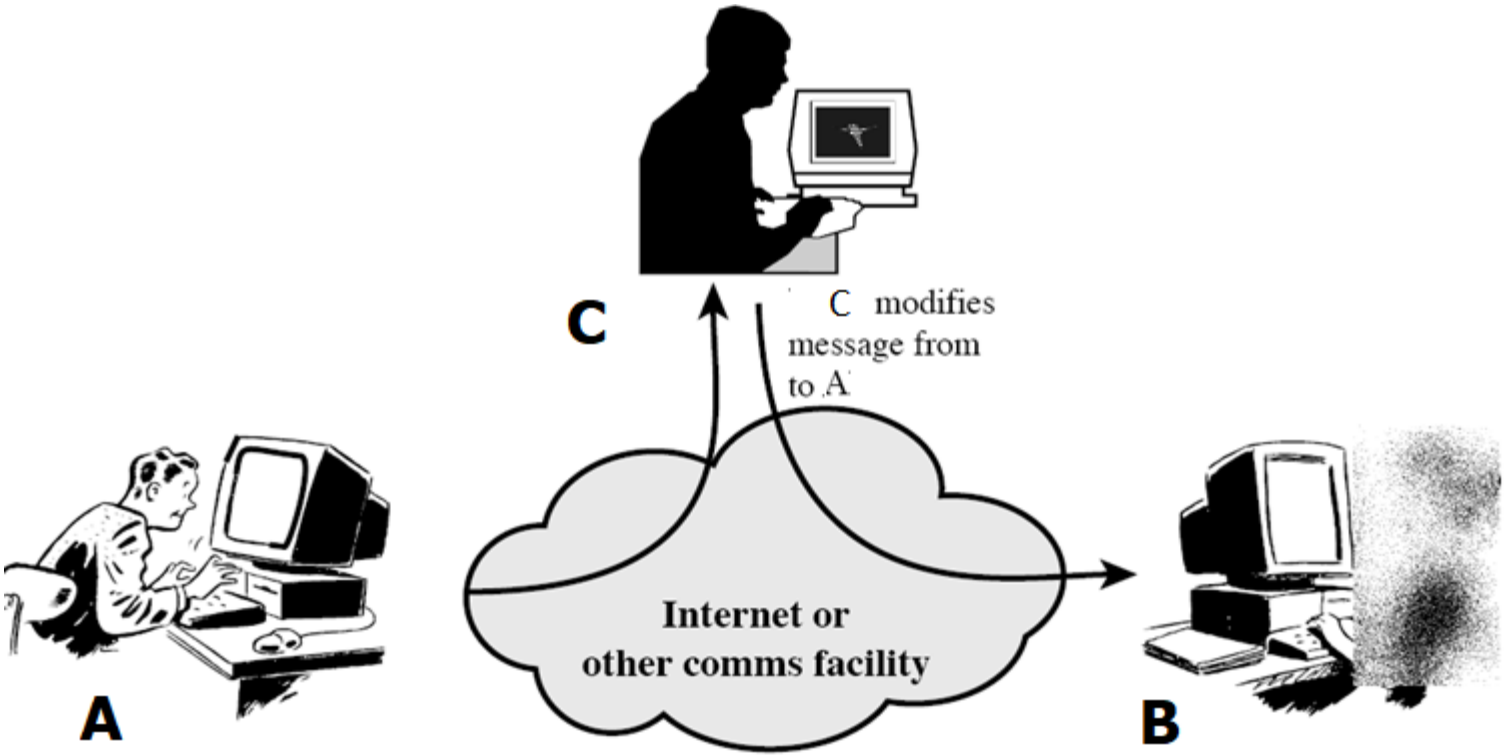
Active Attacks



(b) Replay

التقاط البيانات لإعادة الإرسال مره أخرى

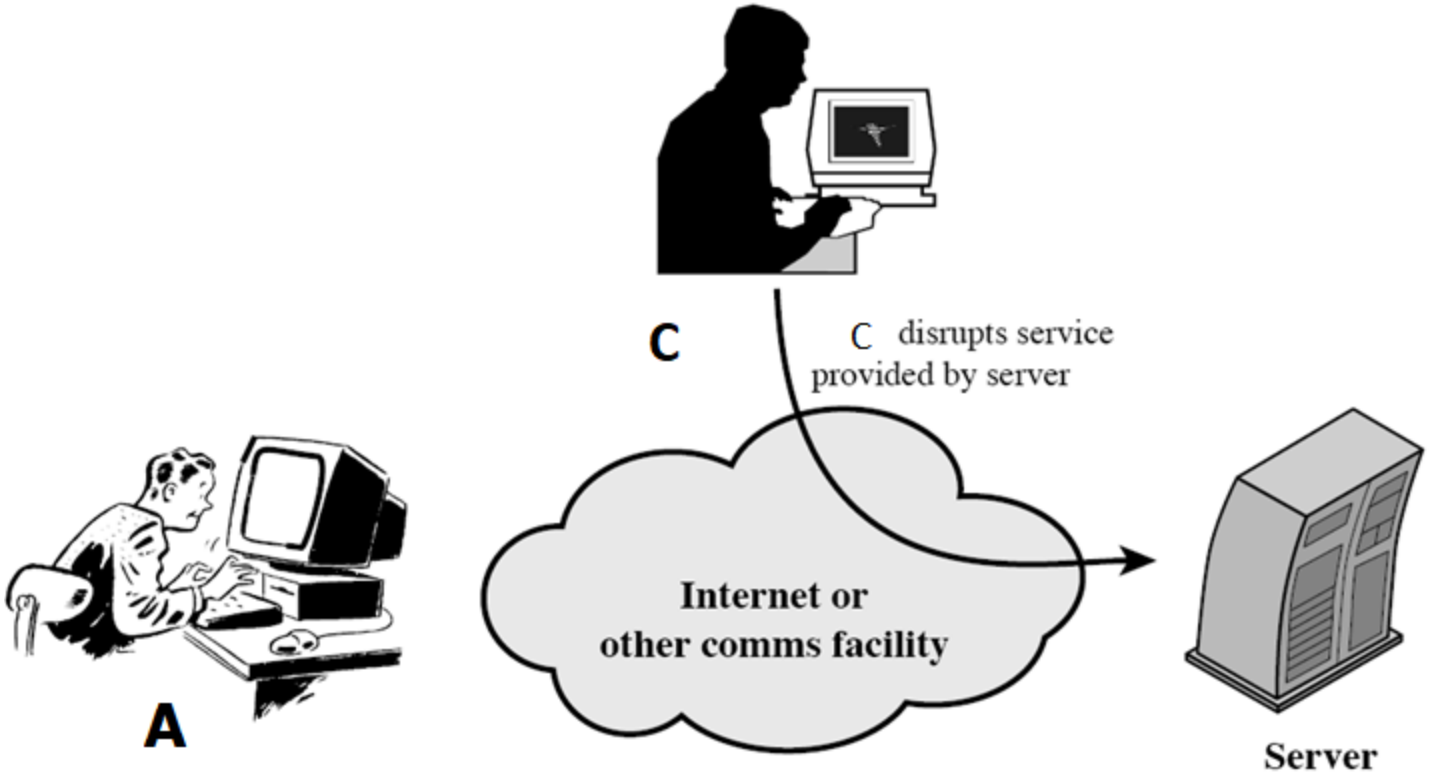
Active Attacks



(c) Modification of messages

يتم تغيير جزء من الرسالة الموثقة

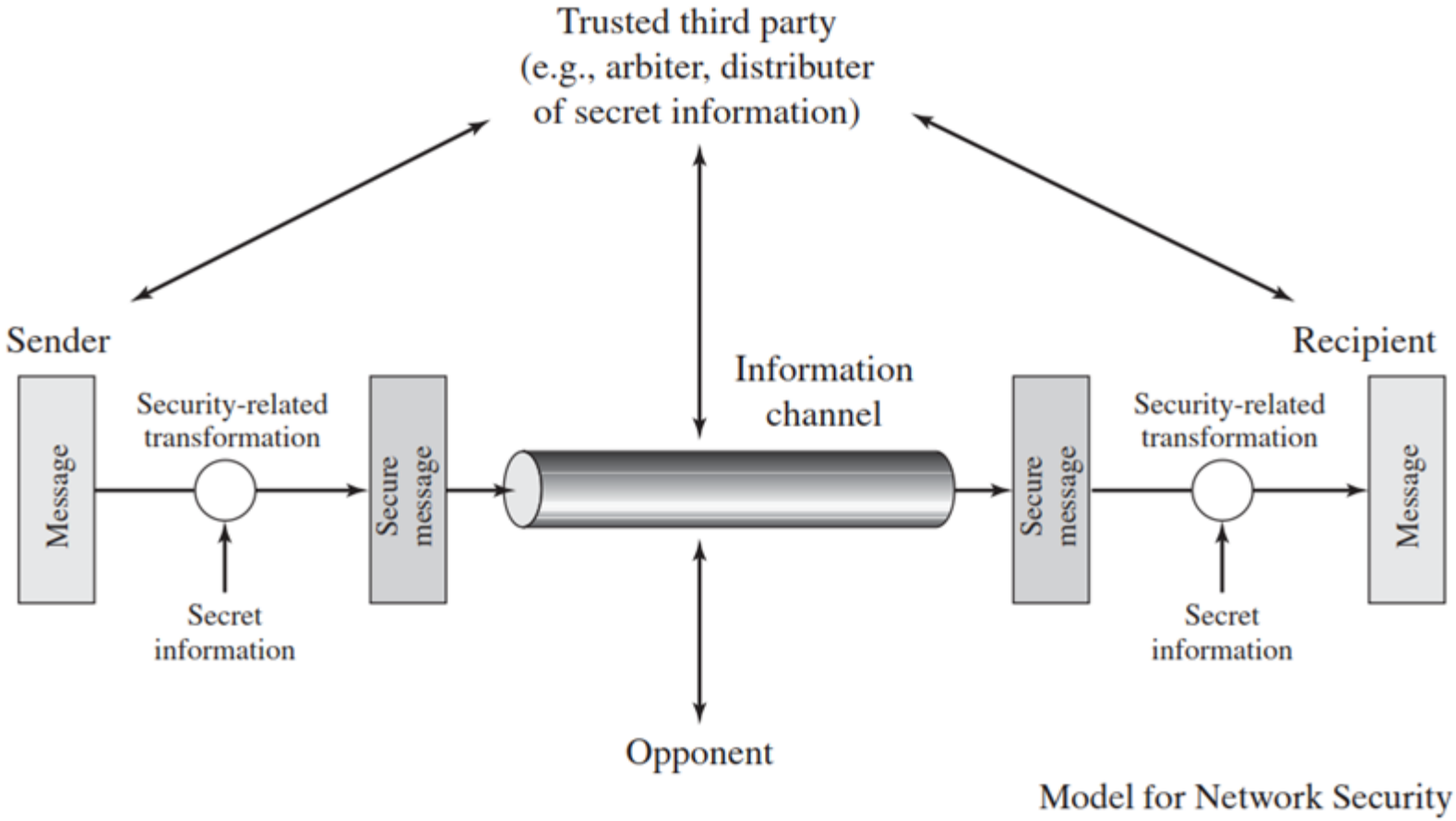
Active Attacks



(d) Denial of service

تعطيل الشبكة عن طريق التعطيل أو التحميل الزائد

Model for Network Security
نموذج لأمن الشبكات



Model for Network Security

Model for Network Security
نموذج لأمن الشبكات

There are four basic tasks in designing a particular security service

هناك أربع مهام أساسية في تصميم خدمة أمنية معينة

1. Design an algorithm for performing the security-related transformation.

تصميم خوارزمية لإجراء التحول المتعلق بالأمان.

2. Create the secret information to be used with the algorithm

إنشاء المعلومات السرية لاستخدامها مع الخوارزمية

3. Develop methods for the distribution and sharing of the secret information

تطوير أساليب لتوزيع وتبادل المعلومات السرية

4. Specify a protocol to be used by the users.

تحديد بروتوكول لاستخدامه بين المستخدمين.

Cyber Security

Cyber Security

- Cyber security is the practice of defending **computers**, **servers**, **mobile devices**, **electronic systems**, **networks**, and **data** from malicious attacks.

الأمن السيبراني هو ممارسة الدفاع عن أجهزة الكمبيوتر والخوادم والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات من الهجمات الضارة

- It's also known as **information technology security** or **electronic information security**.
- تعرف أيضا باسم أمن تكنولوجيا المعلومات أو أمن المعلومات الإلكترونية.

Categories of Cyber Security

Categories of Cyber Security

- The categories of Cyber Security:

1. Network security is securing a computer network from intruders, whether attackers or malware.

هي ممارسة تأمين شبكة كمبيوتر من المتسللين، سواء كانوا مهاجمين أو برامج ضارة.

2. Application security focuses on keeping software and devices free of threats. Successful security begins in the design stage.

يركز على الحفاظ على البرامج والأجهزة خالية من التهديدات. يبدأ الأمان الناجح في مرحلة التصميم.

3. Information security protects the integrity and privacy of data, both in storage and in transit.

يحمي سلامة وخصوصية البيانات، سواء في التخزين أو في النقل.

Categories of Cyber Security

4. Operational security includes the processes and decisions for handling and protecting data.

يتضمن العمليات والقرارات الخاصة بمعالجة البيانات وحمايتها

5. Disaster recovery and business continuity

التعافى من الكوارث واستمرارية الأعمال

define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data.

تحديد كيفية استجابة المنظمة لحادث الأمن السيبراني أو أي حدث آخر يتسبب في فقدان العمليات أو البيانات.

Categories of Cyber Security

6. End-user education

addresses the most unpredictable cyber-security factor: people.

يعالج أكثر عوامل الأمن السيبراني التي لا يمكن التنبؤ بها: الأشخاص.

Anyone can by mistake introduce a virus to a secure system. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons are vital for the security of any organization.

يمكن لأي شخص عن طريق الخطأ إدخال فيروس إلى نظام آمن. يعد تعليم المستخدمين حذف مرفقات البريد الإلكتروني المشبوهة ، وعدم توصيل محركات أقراص USBمجهولة الهوية ، والعديد من الدروس المهمة الأخرى أمرا حيويا لأمن أي مؤسسة.

Importance of Cyber Security

أهمية الأمن السيبراني

Importance of Cyber Security
أهمية الأمن السيبراني

- Cyber attacks affect all people.

تؤثر الهجمات السيبرانية على جميع الناس.

- The fast changes in technology will cause a boom in cyberattacks.

التغييرات السريعة في التكنولوجيا سوف تسبب طفرة في الهجمات السيبرانية.

- Damage to businesses and loss of jobs.

الأضرار التي لحقت بالشركات وفقدان الوظائف.

- Cyber security threats faced by individuals.

تهديدات الأمن السيبراني التي يواجهها الأفراد.

- Cyber concerns may result in increased regulations and legislation.

قد تؤدي المخاوف السيبرانية إلى زيادة اللوائح والتشريعات.

Types of Cyber Threats

أنواع التهديدات السيبرانية

Types of Cyber Threats
أنواع التهديدات السيبرانية

- The threats countered by cyber-security are three-fold:

التهديدات التي يواجهها الأمن السيبراني هي ثلاثة أوجه:

1. **Cybercrime** **الجرائم السيبرانية**

Includes single actors or groups targeting systems for financial gain or to cause disruption.

الجرائم السيبرانية تشمل جهات فاعلة فردية أو مجموعات تستهدف الأنظمة لتحقيق مكاسب مالية أو للتسبب في اضطراب.

2. **Cyber-attack** **الهجوم السيبراني**

Involves politically motivated information gathering. يشمل جمع المعلومات بدوافع سياسية.

3. **Cyberterrorism** **الإرهاب السيبراني**

Intended to undermine electronic systems to cause panic or fear.

هدف إلى تقويض الأنظمة الإلكترونية لتسبب الذعر أو الخوف.

Types of Cyber Threats

- **Some of the common methods used to threaten cyber-security:**

بعض الطرق الشائعة المستخدمة لتهديد الأمن السيبراني:

- Malware such as Virus, Trojans, Spyware, Ransomware, Adware, and Botnets.

البرامج الضارة مثل الفيروسات وأحصنة طروادة وبرامج التجسس وبرامج الفدية والبرامج الإعلانية وشبكات الروبوتات.

- SQL Injection — حقن لغة قاعدة البيانات
- Phishing — التصيد
- Man-in-the-Middle attack — الهجوم فى المنتصف
- Denial-of-service attack — هجوم الحرمان من الخدمة

Expected outputs after teaching this course

المخرجات المتوقعة بعد تدريس هذا المقرر

Expected Output of Course

- The need for Cyber Security. الحاجة إلى الأمن السيبراني
- Data Encryption and Decryption Techniques.

تقنيات تشفير البيانات وفك تشفيرها.

- Attacks, Concepts, and Protecting.

الهجمات والمفاهيم والحماية

- Data Privacy and Data Consistency

خصوصية البيانات وتقارب البيانات

- Will your future be in Cyber Security.

هل سيكون مستقبلك في الأمن السيبراني.