جامعة المنارة الخاصة

كلية الهندسة

هندسة الميكاترونيكس

Information System Security

أمن نظم المعلومات

مدرسة المقرر

د. بشرى علي معلا

عناوين المحاضرة الأولى

- مقدمة
- تعريف أمن المعلومات
- العلاقة بين مفهومي الأمن والشبكة
- أنواع التحكم بأمن المعلومات
- متطلبات أمن المعلومات
- مفهوم الهجمات وتصنيفها
- نموذج أمن الشبكة
- الجدران النارية

مقدمة

- مع ظهور شبكة الانترنت واتساع نطاق استخدامها بدأت تظهر مشكلة ضعف السرية في نقل المعلومات والبيانات عبر هذه الشبكة.

- مما زاد من سخونة قضية أمن المعلومات هو انتشار ظاهرة كسر شيفرة بطاقات الائتمان والوصول إلى المصارف والمؤسسات الأمنية الحيوية.

- من هنا جاءت أهمية توفير الأمن للمعلومات بالحفاظ على سريتها، وعدم العبث بمحتواها

مفهوم أمن المعلومات (Information Security)

- هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء.

- أي هو العلم الذي يبحث في التقنيات التي تمنع الحصول على المعلومات و/أو تعديلها إلا من قبل المخّول لهم بذلك.

- **عرفت لجنة أنظمة الأمن القومي Committee on National Security Systems (CNSS) أمن المعلومات بأنه: حماية المعلومات وكل المكونات الحرجة من الأنظمة و التجهيزات الصلبة التي تستخدم أو تختزن أو ترسل تلك المعلومات.**

العلاقة بين مفهومي الأمن و الشبكة

الأمن

اتصالات مغلقة

(Closed Communication)

وصول مقيد

Full Lockdown

شبكة

اتصالات مفتوحة

(Open Communication)

وصول كامل

Full Access

يجب تحقيق التوازن بين المفهومين

أنواع التحكم بأمن المعلومات (1/3)

- يوجد ثلاث فئات أساسية للتحكم بأمن المعلومات:

1. فيزيائي:

يمثل المكونات المادية التي تؤمن الحماية من اللصوص والمخربين، مثال استخدام أجهزة كالأقفال و كاشفات الحركة..

أنواع التحكم بأمن المعلومات (2/3)

- يوجد ثلاث فئات أساسية للتحكم بأمن المعلومات:

2. منطقي

يمثل برمجيات التحكم بالوصول، البرمجيات المضادة للفيروسات، كلمات المرور والبطاقات الذكية.

أنواع التحكم بأمن المعلومات (3/3)

- يوجد ثلاث فئات أساسية للتحكم بأمن المعلومات:

3. إداري:

يتعلق بالإجراءات المرتبطة بالأشخاص والخاصة بإدارة سلوك الأفراد، وهو يشمل التدريب على محددات الأمن وتقييم الأداء ...

متطلبات أمن المعلومات
(Security Requirements)

1. الموثوقية /السرية (Confidentiality/Privacy)
2. تكاملية المعطيات (Data Integrity)
3. المصادقة (Authentication)
4. التحكم بالوصول (Access Control)
5. التوافرية (Availability)
6. الترخيص / التفويض (Authorization)
7. عدم التنصل (Non-Repudiation)

الموثوقية/السرية
(Confidentiality/Privacy)

- تسمح بالحماية من الإطلاع غير الشرعي على المعلومات من قبل غير المخول لهم بذلك.

أي : السماح للأشخاص الشرعيين فقط بالوصول إلى المعلومات المخول لهم الحصول عليها: مثلاً، في الخدمات المدفوعة (التلفزيون باستخدام الانترنت، التعليم عن بعد، ..)، يحق فقط للأشخاص الذين دفعوا الحصول على الخدمة

- يعد التشفير من أكثر الطرائق شيوعاً لضمان سرية المعلومات.

تكاملية المعطيات

Data Integrity

- ✓ تسمح بالتحقق من أن المعطيات لم يطرأ عليها أي تعديل من قبل أي كيان غير مخول له بذلك سواء بشكل مفاجئ أو مقصود.
- ✓ يمكن التعديل بالطرائق المسموحة ومن قبل المفوضين بذلك فقط.
- ✓ من طرائق ضمان تكاملية المعطيات : تقنيات الترميز، التواقيع الرقمية، توابع البعثرة، برمجيات التحري عن الفيروسات واكتشافها ...

المصادقة

Authentication

- ✓ تسمح بالتحقق من هوية الكيان أو المصدر الذي يرسل الرسالة
- ✓ طريقة المصادقة الأكثر بساطة هي:
  استخدام الزوج: اسم المستخدم/كلمة المرور

التو افرية
(Availability)

- التأكد من **استمرار** عمل النظام المعلوماتي، أي استمرار القدرة على التفاعل مع المعلومات، تقديم الخدمة وضمان وصول الأشخاص المخولين إلى المعلومات عندما يريدون.

أمثلة توضح الفرق بين المفاهيم الثلاث السابقة(1/2)
(Confidentiality, Integrity, Availability)

- مثال1: سرقة نسخة من ملف غير مشفر
  - الوثوقية Confidentiality: غير محققة لأن الملف لم يعد سرياً
  - التكاملية Integrity: محققة لأنه لم تجر أي عملية تعديل
  - التو افرية Availability: محققة لأن الملف لا يزال متاح ويستطيع المستخدمين الوصول إليه
- مثال2: إرسال ملف فيه معلومات مزيفة
  - الوثوقية Confidentiality: محققة لأن الملف بقي سرياً
  - التكاملية Integrity: غير محققة لأنه تم حشر معلومات غير صحيحة ضمن الملف
  - التو افرية Availability: محققة لأن الملف لا يزال متاح ويستطيع المستخدمون الوصول إليه

أمثلة توضح الفرق بين المفاهيم الثلاث السابقة(2/2)
(Confidentiality, Integrity, Availability)

- مثال 3 إخفاء ملف شخص ما

  - الوثوقية Confidentiality: محققة لأن الملف بقي سرياً
  - التكاملية Integrity: محققة لأنه لم تجر أي عملية تعديل
  - التو افرية Availability: غير محققة لأن الملف لم يعد متاحاً

التحكم بالوصول
(Access Control)

✓ تسمح بالتحقق من أن أي كيان لا يمكن له الوصول **إلا إلى** الخدمات والمعلومات المسموحة .

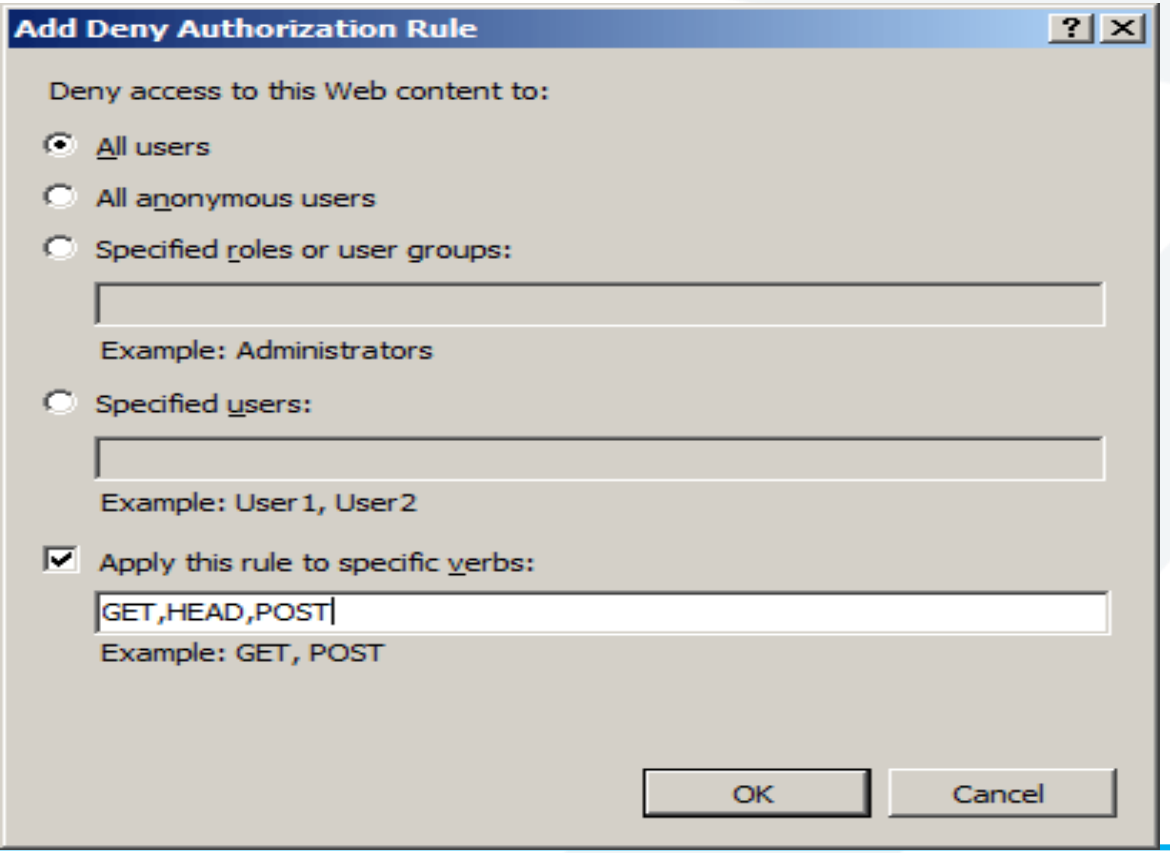
التحكم بالوصول هو أسلوب ينظم مَنْ وماذا يمكن عرضه أو استخدامه من الموارد في نظام ما

أي : تحدد مستوى الوصول المسموح به لكل مستخدم

✓يرتبط غالباً بالمصادقة: فبعد أن تنفذ عملية المصادقة يقوم النظام بتحديد ما هو مسموح به، وبذلك يتجنب المستخدمين غير المفوض/المخول لهم بالوصول إلى البيانات.

الترخيص/ التفويض
(Authorization)

- ✓ عملية الحصول على تفويض للوصول إلى مستوى معين
- ✓ تشمل أنواع حقوق الوصول في نظام الملف الممنوحة في عملية الترخيص :



--> قراءة: السماح بقراءة الملفات أو عرض محتويات المجلدات.

--> كتابة: السماح بالكتابة في الملفات أو بإضافة ملفات إلى المجلدات.

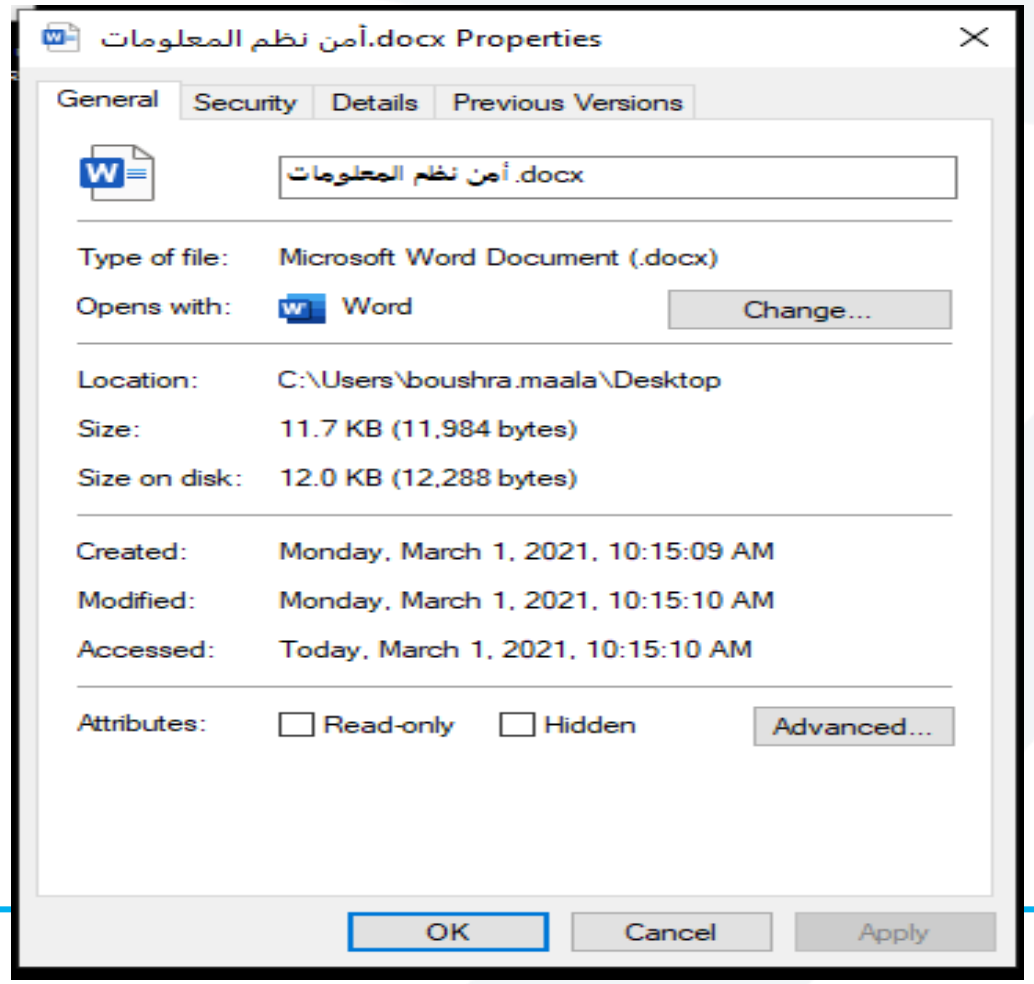
--> تنفيذ: السماح بتنفيذ برنامج ما.

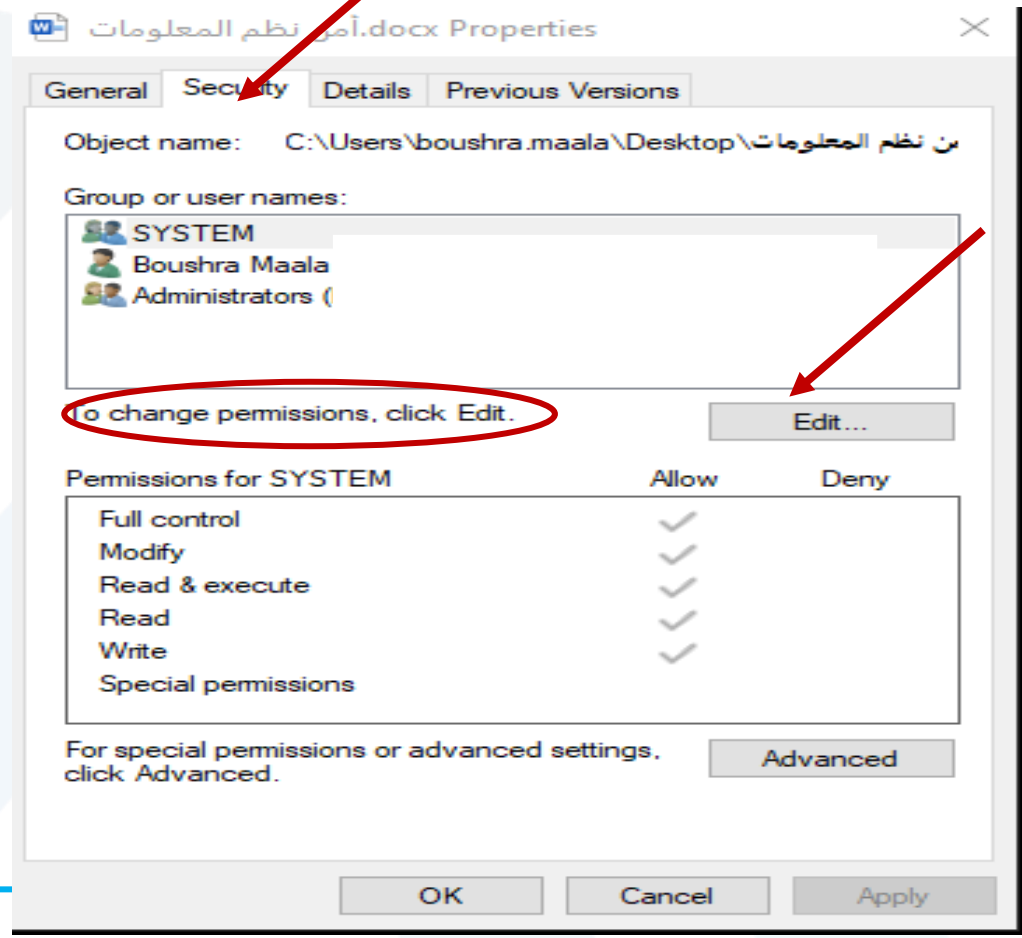
--> إضافة: السماح بإضافة بيانات إلى الملفات أو وضع مجلدات فرعية ضمن مجلدات أخرى.

--> حذف: السماح بحذف ملفات أو مجلدات.

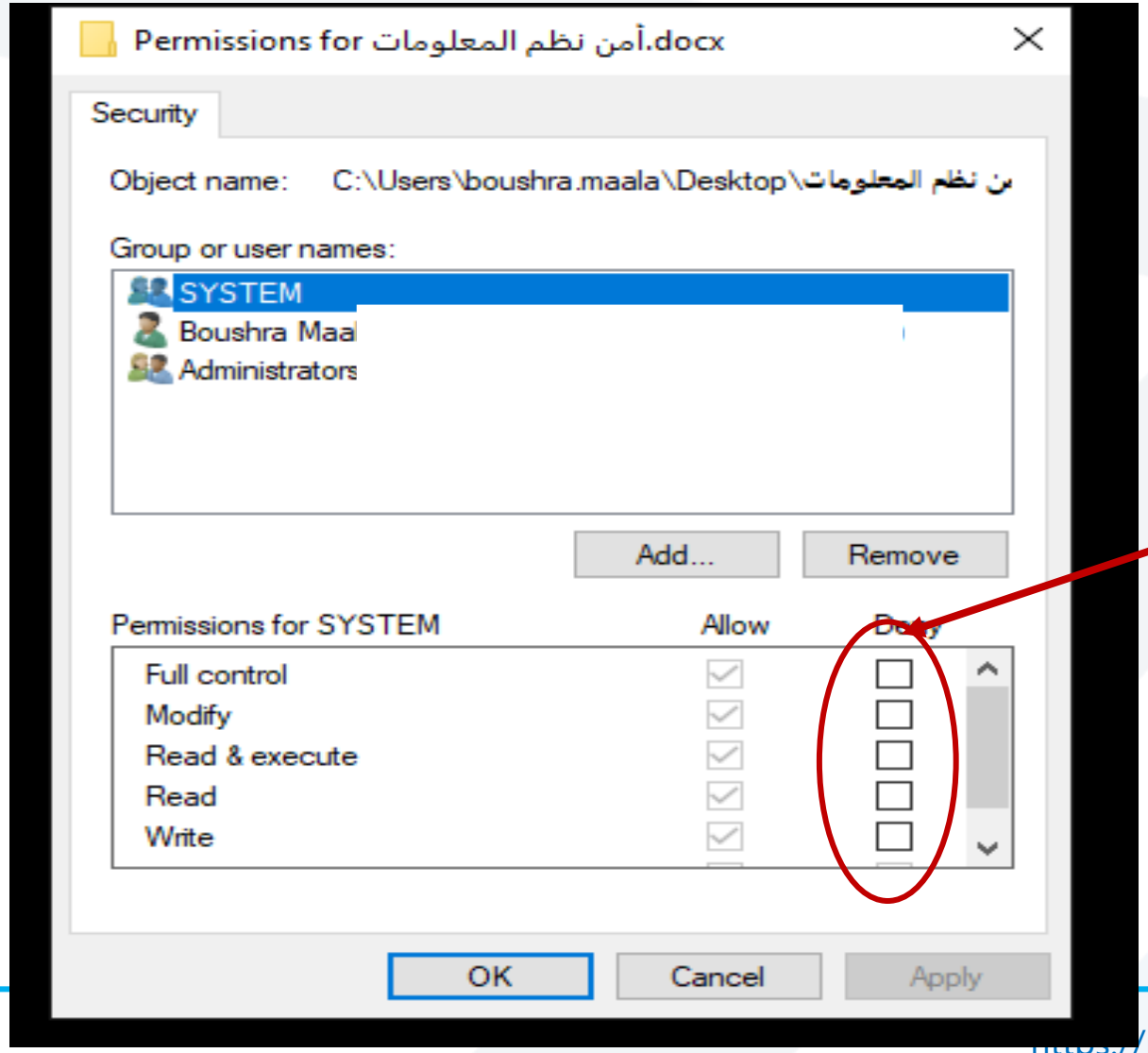
❖ مثال عن التفويض (Authorization) في ملف وورد

✓ نضغط بالزر اليميني على الملف ونختار من القائمة المنسدلة خصائص (properties)





الترخيص/ التفويض
(Authorization)



من هنا يمكن أن نضع السماحيات التي نريدها

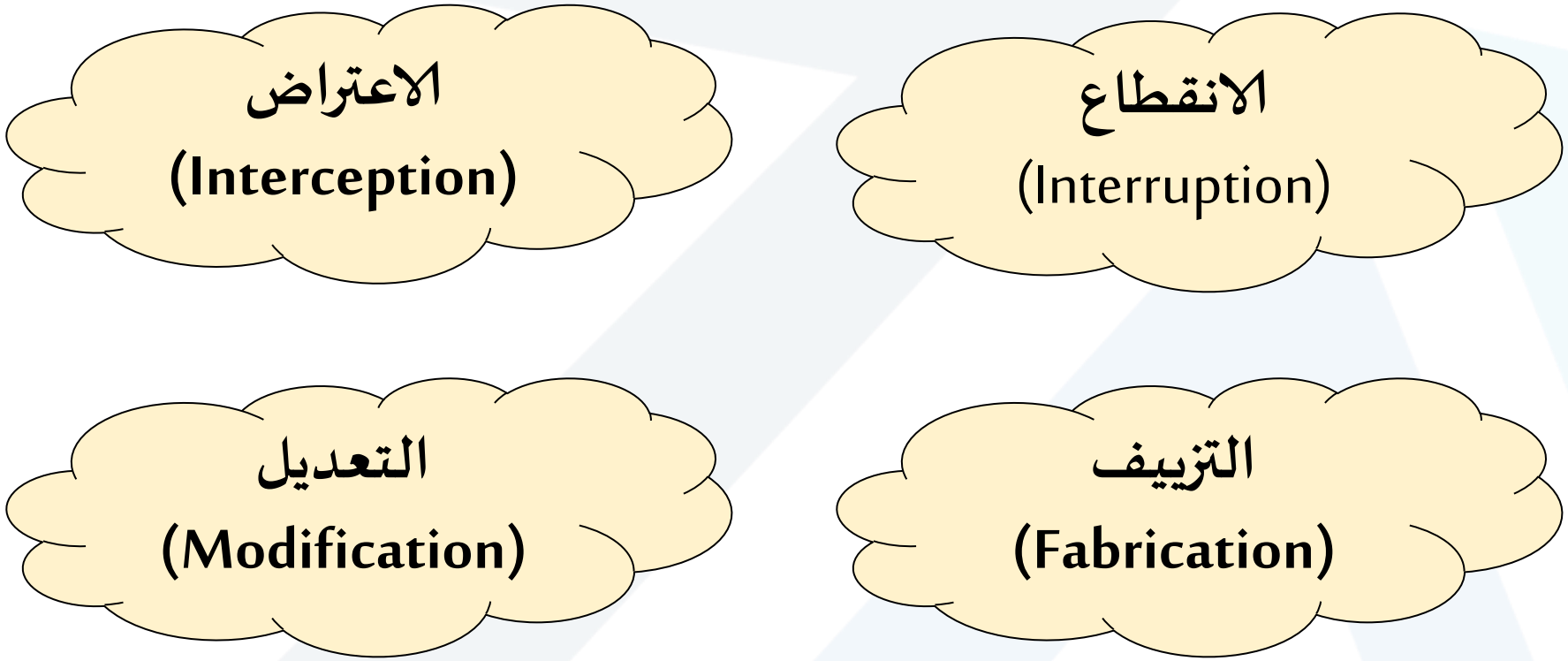
عدم التنصل
(Non-Repudiation)

- ✓ تسمح بالحماية من إنكار الاستقبال أو الإرسال في حالة الاتصال.
- ✓ تهدف إلى ضمان عدم قدرة المستخدم على إنكار أنه هو الذي قام بالتصرف، وهي ذات أهمية بالغة في بيئة الأعمال الإلكترونية والتعاقدات (التجارة الإلكترونية) (عملية التحقق والتأكد من التواقيع)
- ✓ عملية تعريف المستخدمين بطريقة لا يستطيعون معها في وقت لاحق إنكار اشتراكهم في المداولة أو العقد، وذلك عن طريق طرف ثالث موثوق به.

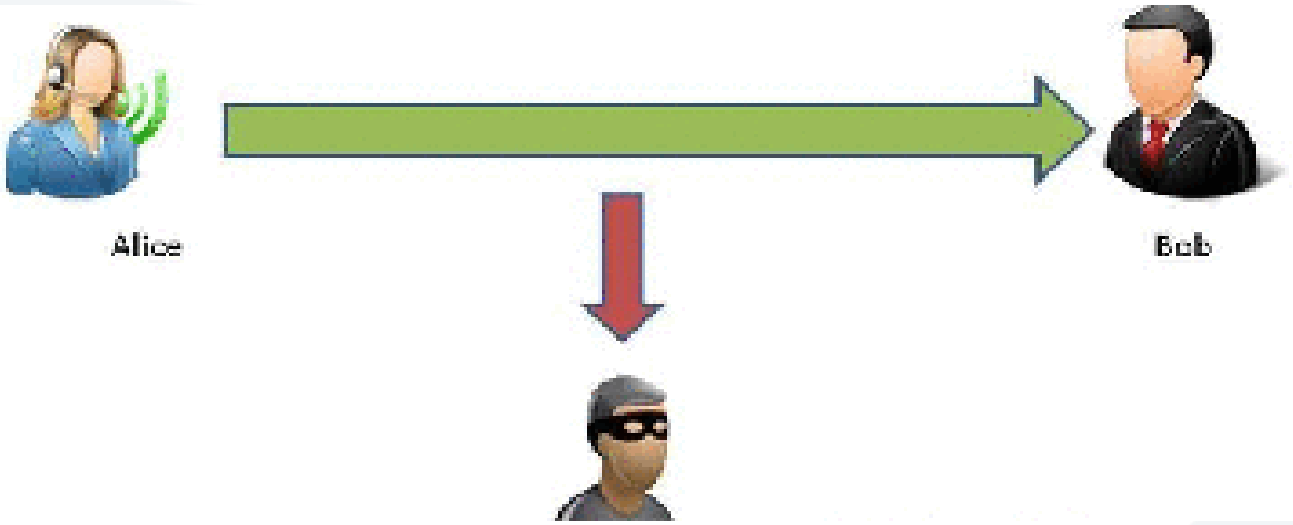
تعد عناصر الموثوقية والتكاملية والمصادقة من أهم عناصر أمن المعلومات، وهي تشكل ما يعرف بمثلث CIA ، ويمكن أن تكون هذه العناصر مستقلة عن بعضها البعض أو متداخلة، ويعد إيجاد التوازن الصحيح بين هذه العناصر الثلاثة واحداً من أهم التحديات في مجال السرية وأمن المعلومات

الهجمات ضد الأمن (1/3)

الهجوم هو الاعتداء على أمن النظام ، هذا الهجوم قد يكون بـ:

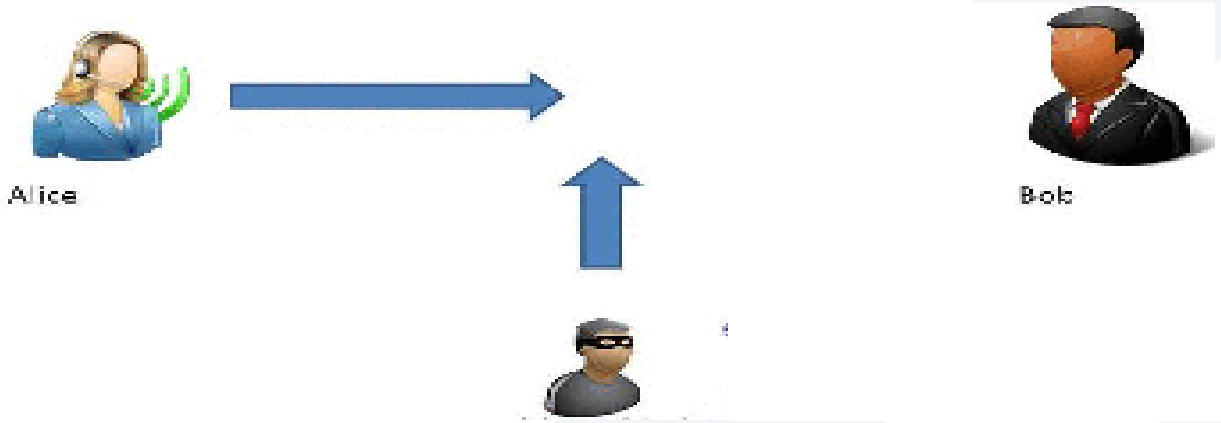


الهجمات ضد الأمن (2/3)



1. الاعتراض (Interception):

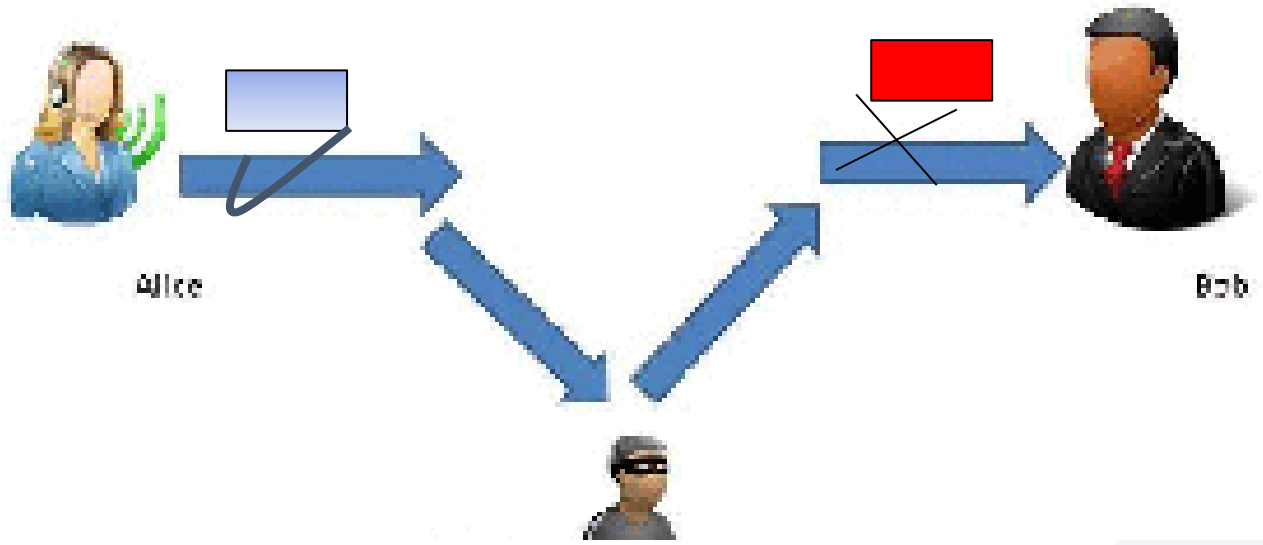
- ✓ أن يستطيع المهاجم الوصول إلى جزء من مكونات النظام غير مسموح له الوصول إليه.
- ✓ يهدد الموثوقية (Confidentiality)



2. الانقطاع (Interruption):

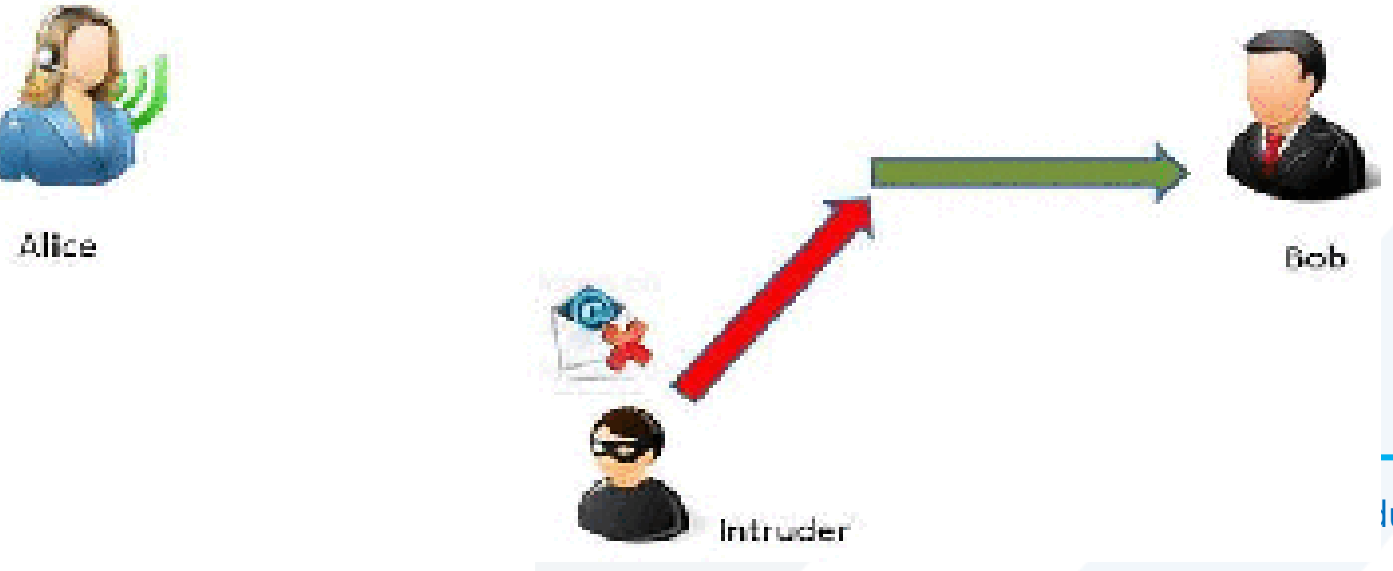
- ✓ أن يدمر المهاجم أحد مكونات النظام بحيث يصبح غير متوفر أو خارج الخدمة . مثلاً قطع الاتصال السلكي ، التشويش على الاتصال اللاسلكي ، إسقاط الرزم.
- ✓ يهدد التوافرية (Availability)

الهجمات ضد الأمن (3/3)



3. التعديل (Modification):

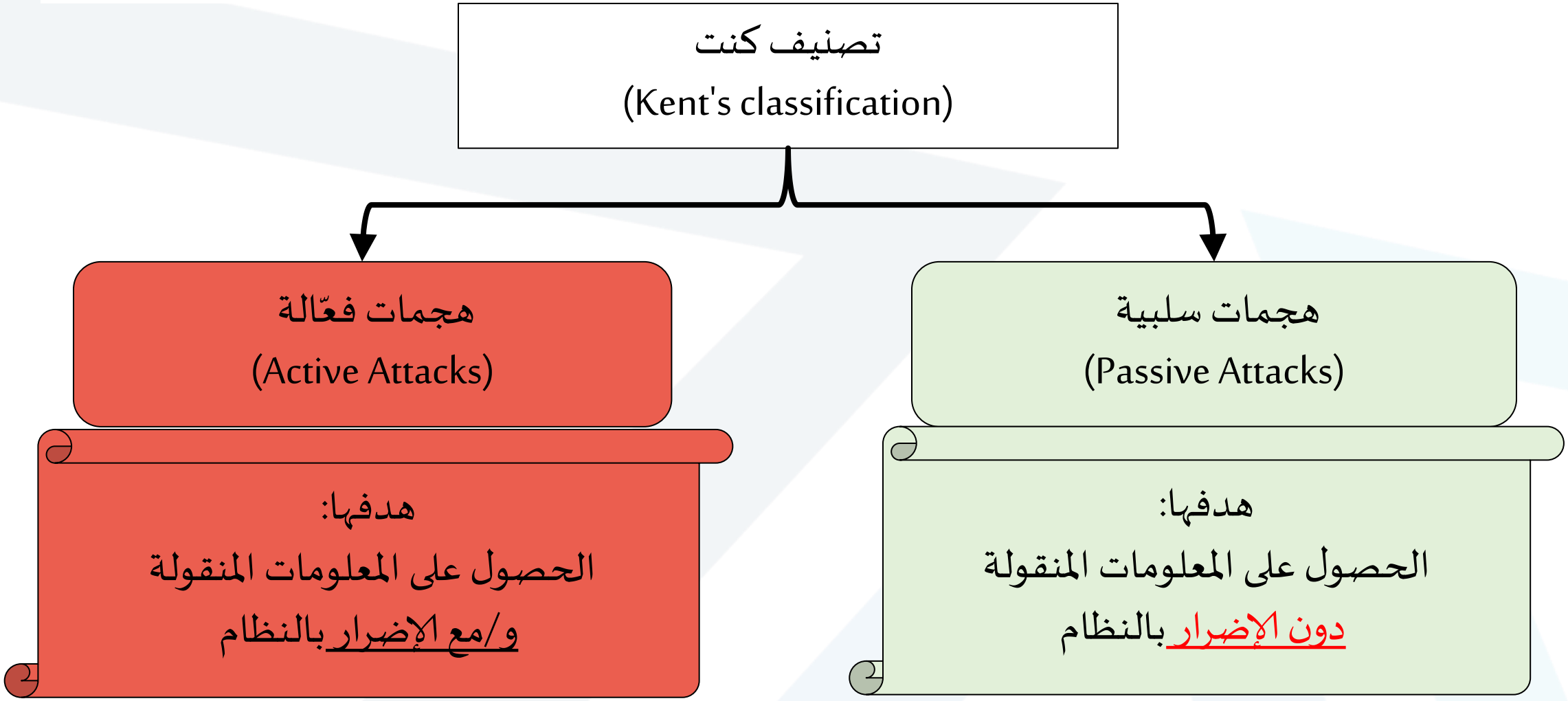
- ✓ أن يستطيع المهاجم الوصول إلى جزء من مكونات النظام غير مسموح له الوصول إليه ويعبث بهذا الجزء.
- ✓ يهدد تكاملية المعلومات (Data integrity)



4. التزييف (Fabrication):

- ✓ أن يحشر المهاجم معلومات مزيفة (أهداف مزيفة) ضمن النظام.
- ✓ يهدد المصادقة (Authentication)

تصنيف الهجمات ضد الأمن



تصنيف الهجمات ضد الأمن (1/6)

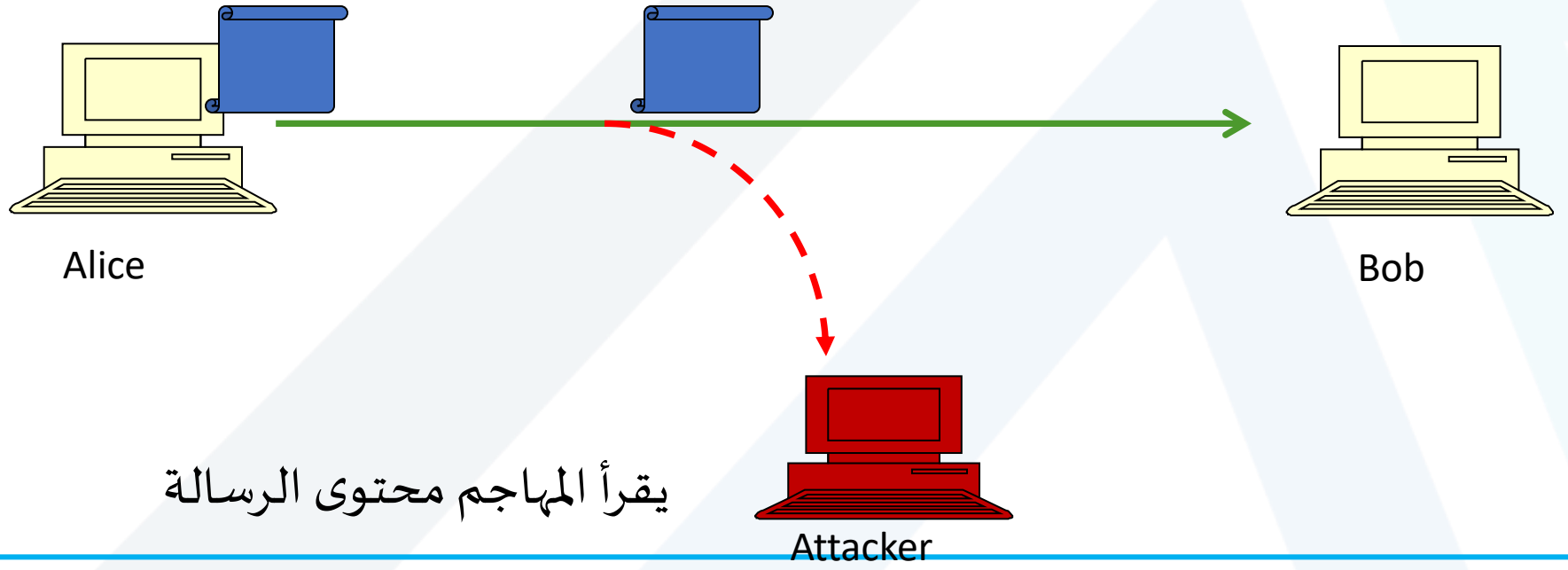
(Security Attacks classification)

❖ الهجمات السلبية :

هي الهجمات التي تتضمن عملية التنصت و مراقبة الإرسال

يوجد نوعان:

1. الحصول على محتوى الرسالة (release of message content)



تصنيف الهجمات ضد الأمن (2/6)

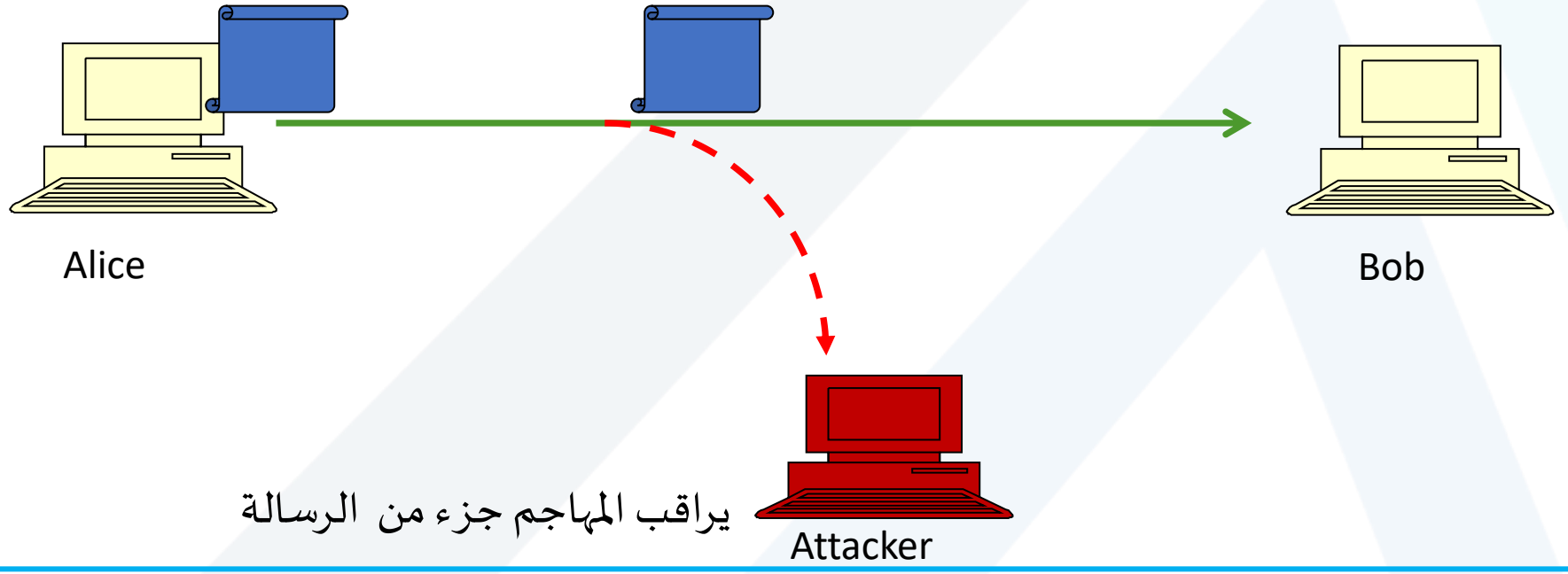
(Security Attacks classification)

❖ الهجمات السلبية :

هي الهجمات التي تتضمن عملية التنصت و مراقبة الإرسال

يوجد نوعان:

2. تحليل حركة المعلومات (Traffic analysis)



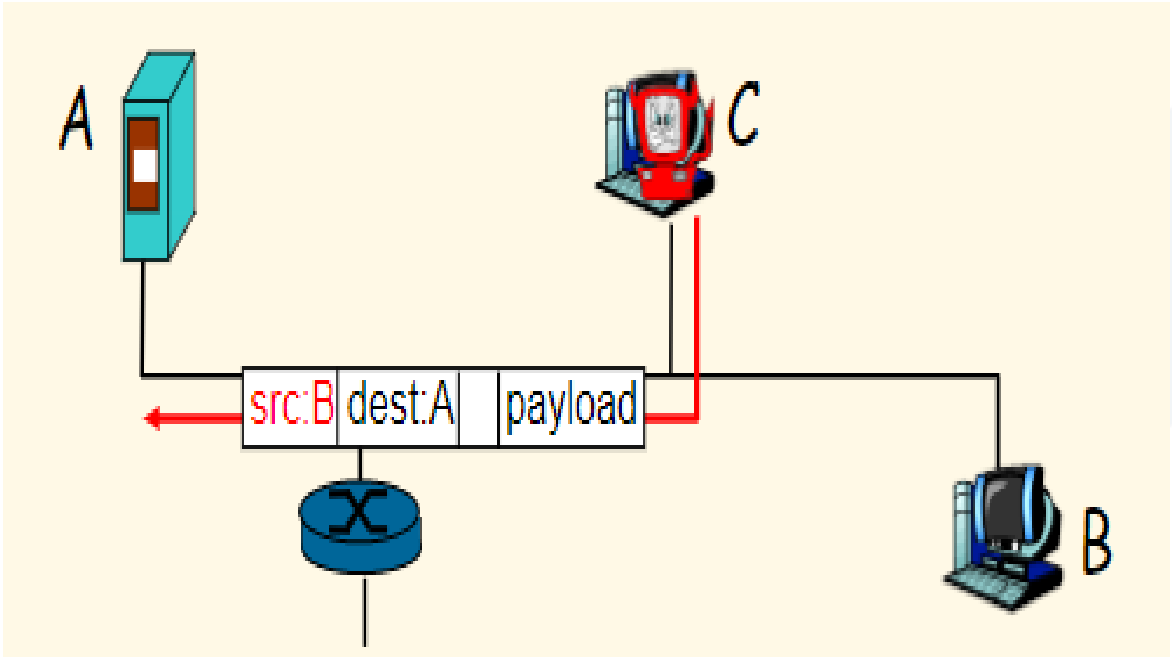
تصنيف الهجمات ضد الأمن (3/6)

(Security Attacks classification)

❖ الهجمات الفعالة:

هي الهجمات التي تتضمن إجراء تعديلات على تدفق المعلومات أو إنشاء رسائل كاذبة

تتضمن أربعة أنواع: 1. التخفي (spoofing-Masquerading) سرقة الهوية



مثال1 :انتحال عنوان الـ IP (IP Spoofing)

يرسل المهاجم رسالة بعنوان IP لعقدة أخرى

مثال : ترسل العقدة C المهاجمة إلى العقدة A على أنها العقدة B

مثال2: الاحتيال على البريد الالكتروني (e-mail Spoofing)

المسؤول المالي

Alice@yourcompany.com

زبون

Bob@yourcompany.com

مهاجم

ينشىء المهاجم بريداً الكترونياً قريباً من البريد الشرعي للمسؤول المالي

البريد الشرعي Alice@yourcompany.com

البريد المزور Alice@yourdomain.com

From: Alice@yourdomain.com

To: Bob@yourcompany.com

Subject: عاجل جداً

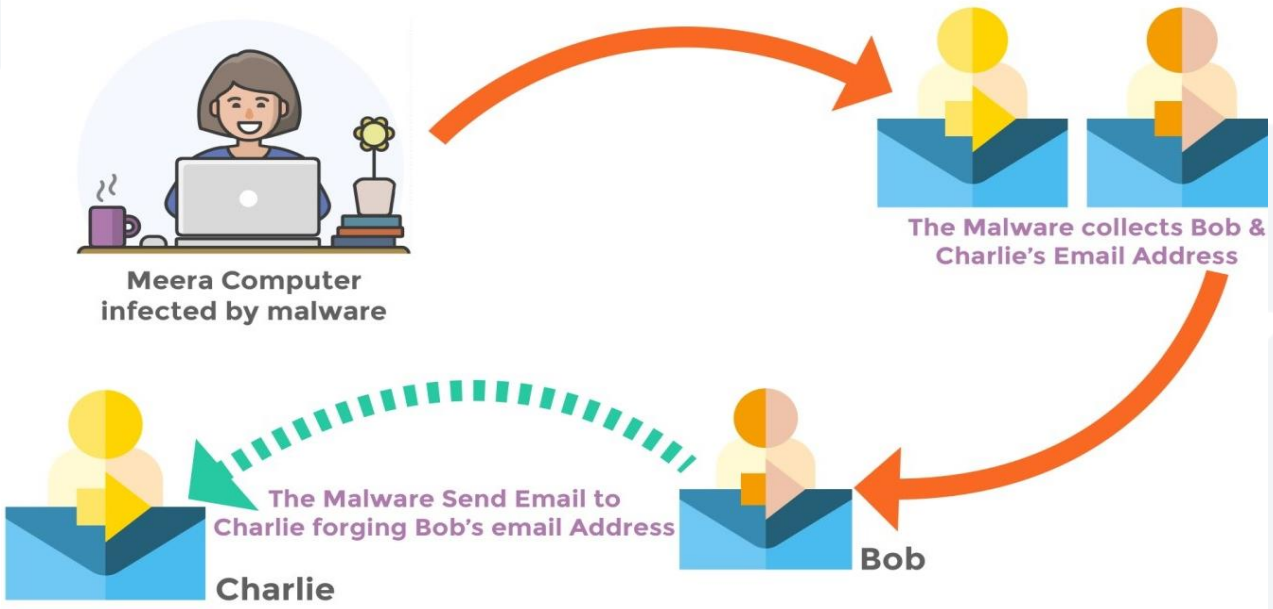
يترتب عليك تحويل مبلغ 50000 $ إلى الحساب الآتي 1211212قبل نهاية اليوم أو تتوقف جميع المعاملات التجارية الجارية حاليا لصالحك.

مهاجم

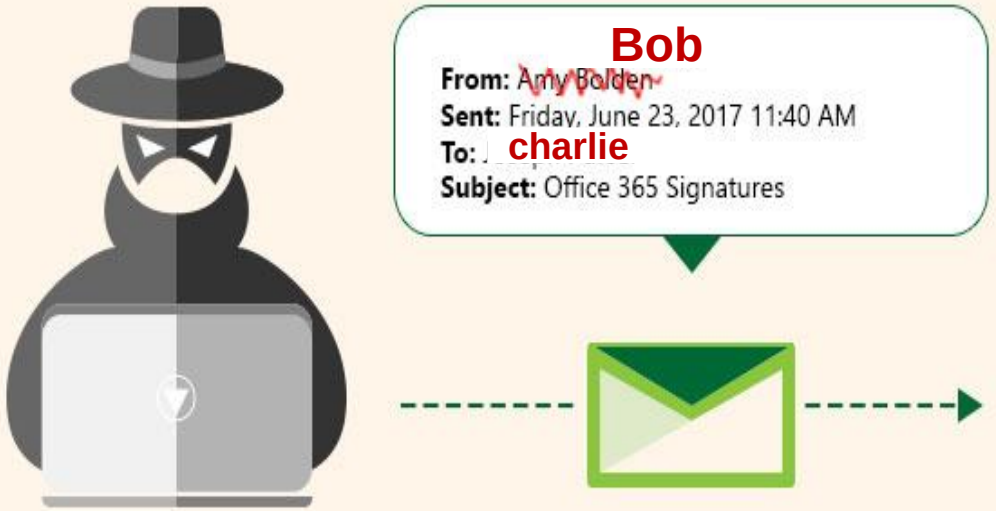
زبون

سيفترض Bob أن الإيميل شرعي وسيقوم بإجراء التحويل

مثال 3 : الاحتيال على البريد الالكتروني (e-mail Spoofing)



- تعرَّض حاسوب ميرا لهجوم ما
- حصل المهاجم على إيميل كل من بوب و شارلي
- يرسل المهاجم إيميل على أنه بوب إلى شارلي



- هذه الطريقة بالهجوم أعقد من المثال السابق
- هناك برامج تسمح للمهاجم أن يضع في جهة المرسل العنوان الذي يريده وليس بالضرورة العنوان الذي يتم منه الإرسال بشكل فعلي.

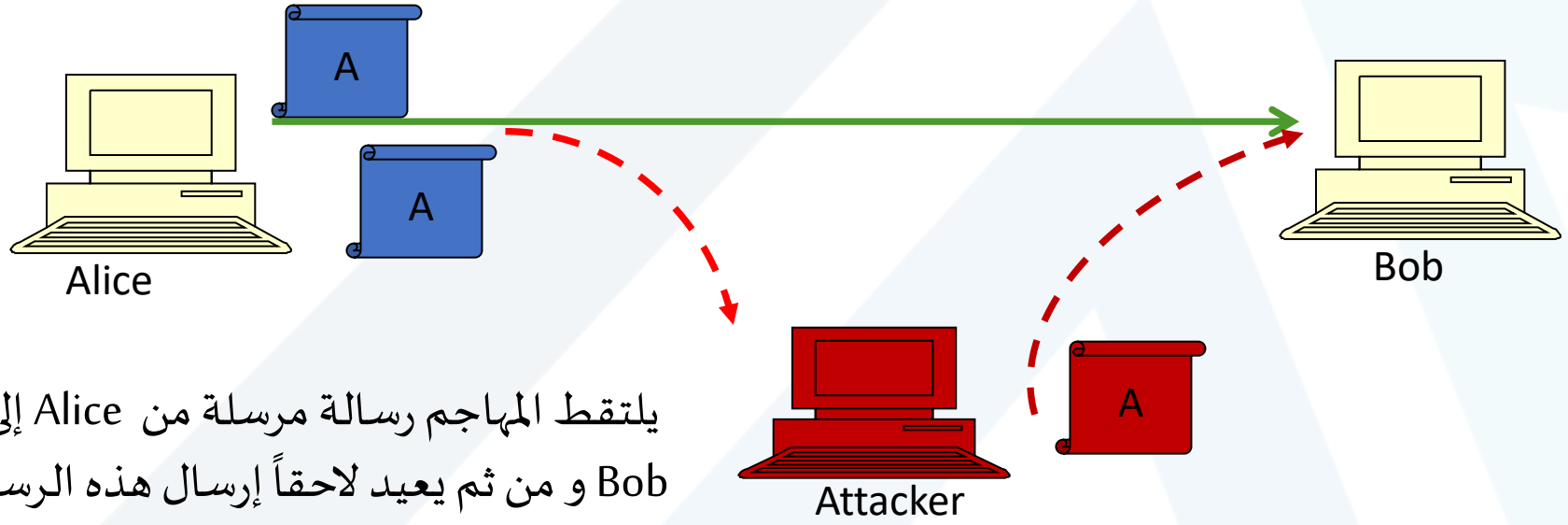
تصنيف الهجمات ضد الأمن (4/6)

(Security Attacks classification)

❖ الهجمات الفعالة:

هي الهجمات التي تتضمن إجراء تعديلات على تدفق المعلومات أو إنشاء رسائل كاذبة

تتضمن أربعة أنواع: 2. إعادة الإرسال (Replay Attack)



يلتقط المهاجم رسالة مرسلة من Alice إلى Bob و من ثم يعيد لاحقاً إرسال هذه الرسالة

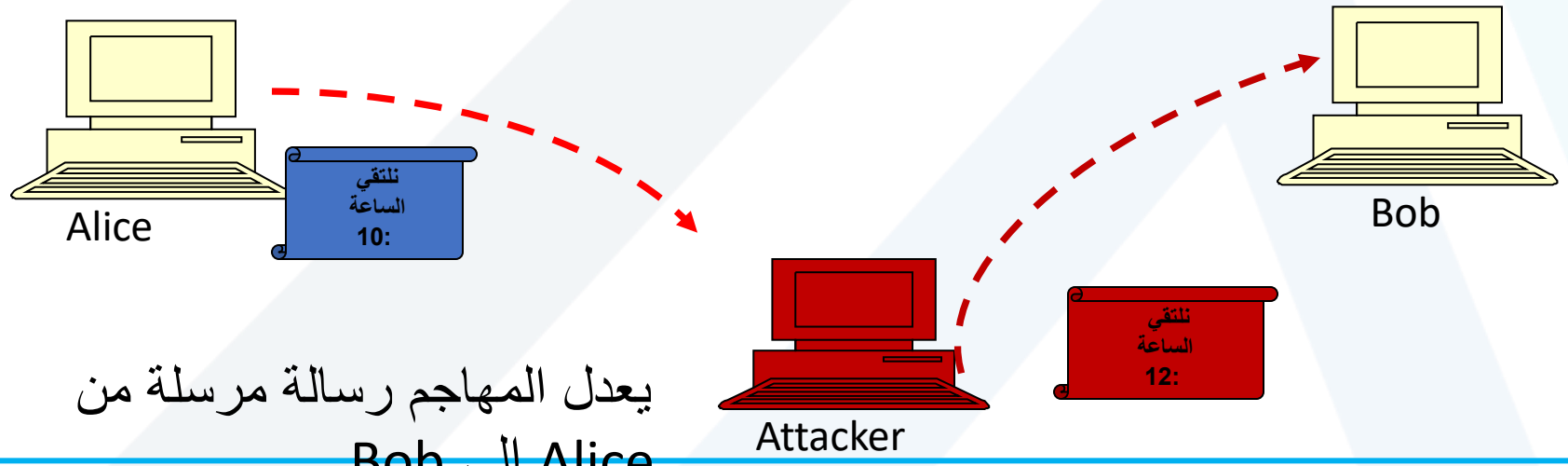
تصنيف الهجمات ضد الأمن (5/6)

(Security Attacks classification)

❖الهجمات الفعالة:

هي الهجمات التي تتضمن إجراء تعديلات على تدفق المعلومات أو إنشاء رسائل كاذبة

تتضمن أربعة أنواع: 3. تعديل الرسائل (Modification of message)



يعدل المهاجم رسالة مرسلة من Alice إلى Bob

تصنيف الهجمات ضد الأمن (6/6)

(Security Attacks classification)

❖ الهجمات الفعالة:

هي الهجمات التي تتضمن إجراء تعديلات على تدفق المعلومات أو إنشاء رسائل كاذبة

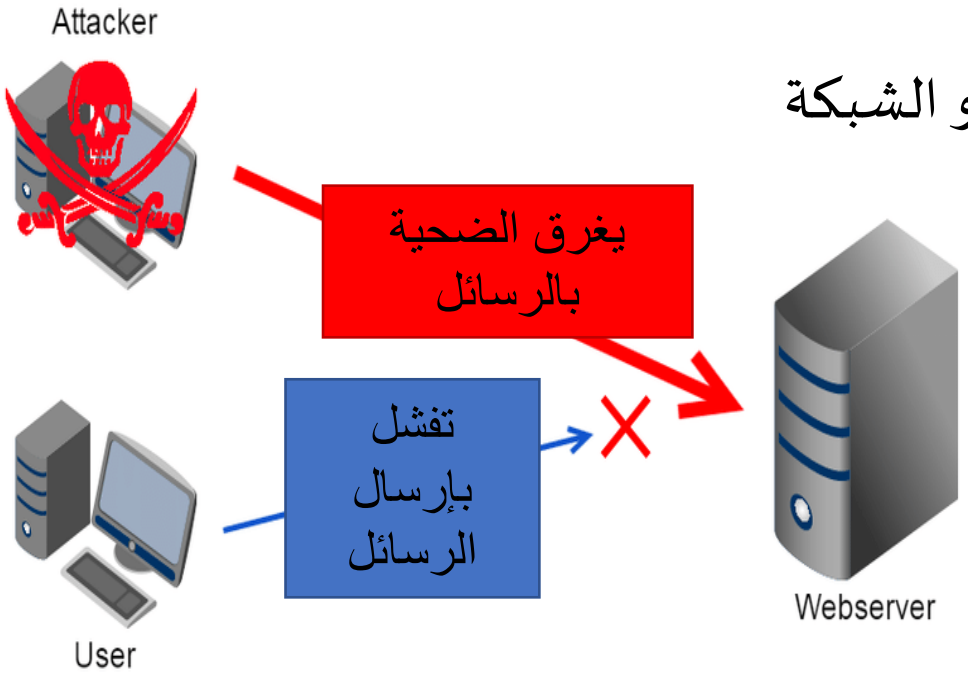
تتضمن أربعة أنواع: 4. حجب الخدمة DoS (Denial of Service)

هدفه:

جعل الخدمة غير متوفرة من خلال التحميل الزائد(overloading) للمخدم أو الشبكة

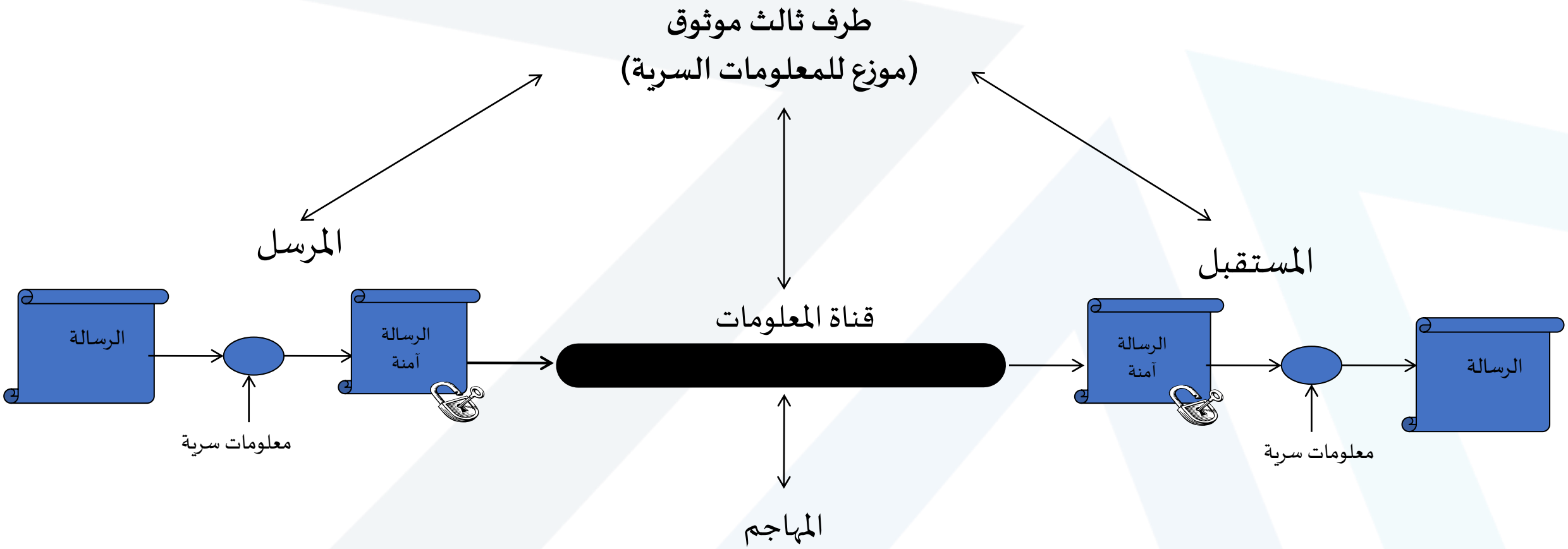
من خلال:

- ✓استنفاذ المصادر في الشبكة
- ✓استنفاذ عرض الحزمة
- ✓.....



نموذج أمن الشبكة

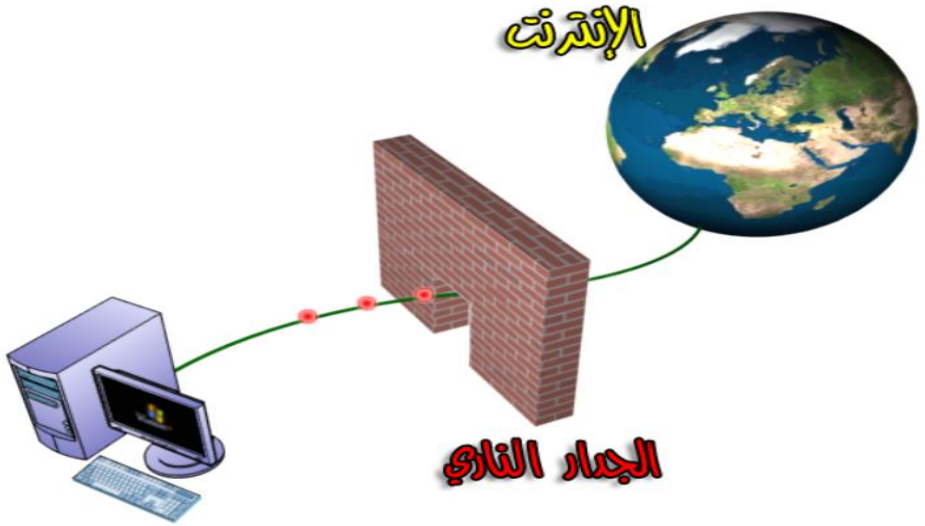
(Security Network Model)



الجدران النارية (1/5)

(Firewalls)

- تستخدم لمنع الوصول غير المصرح به من خارج الشبكة إلى داخلها و من داخل الشبكة إلى خارجها.
- إنه مصمم ليدفع للأمام ببعض الرزم و يمنع بعضها الآخر.



الجدران النارية (2/5)

(Firewalls)

❖ تكون الجدران النارية إما :

✓ برمجيات

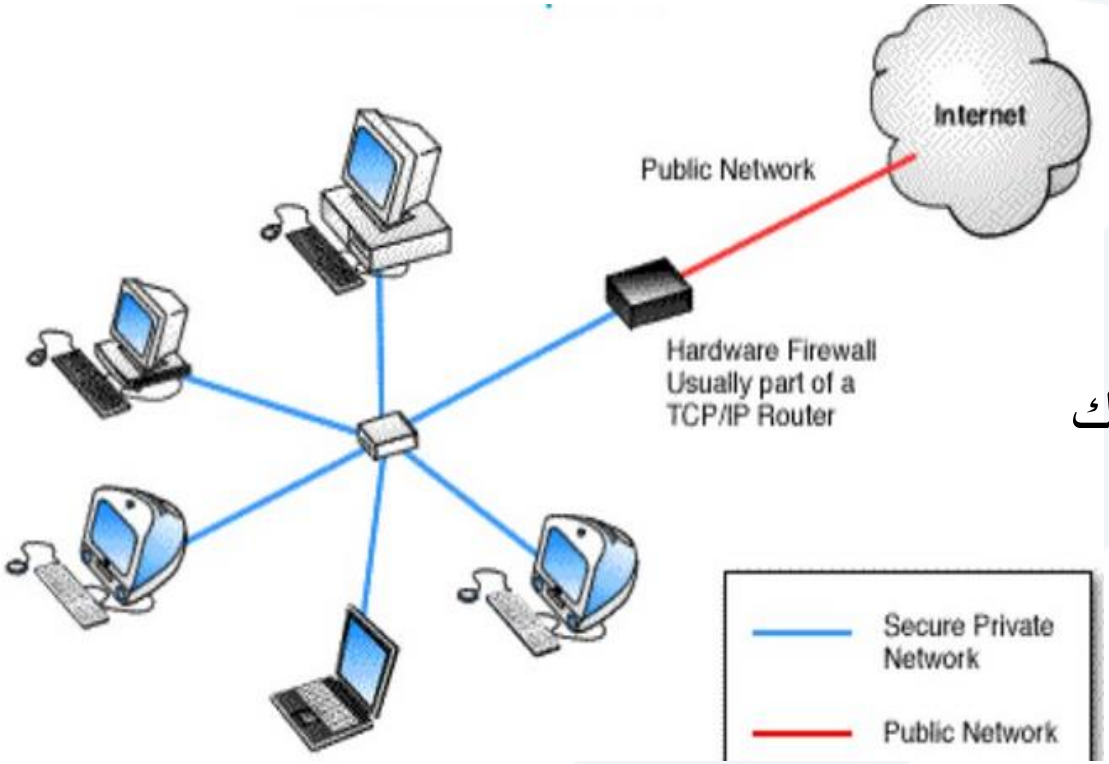
- هي الأرخص والأكثر انتشاراً
- سهلة التنزيل
- لكنها قد تستهلك جزء اً كبيراً من موارد النظام
- وقد تتسبب في مشاكل مع برمجيات أخرى موجودة على الجهاز

الجدران النارية (3/5)

(Firewalls)

❖ تكون الجدران النارية إما :

✓عتاد صلب



- تستخدم بشكل أكبر في الشركات والمؤسسات الكبيرة
- عادة ما تتوضع بين الموجهات واتصال الانترنت
- هي مخصصة من أجل تطبيق وظائف الجدران النارية لذا لا تستهلك من موارد الأجهزة الحاسوبية
- عيبها الأساسي هي الصيانة وذلك لصعوبة تهيئتها وتحديثها بشكل صحيح

الجدران النارية (4/5)

(Firewalls)

❖ يوجد نوعان للجدران النارية حسب آلية عمله:

1. النوع الأول : يعتمد على **أسماء البرامج** لتحديد فيما إذا كانت مسموح لها الاتصال بالانترنت أم لا. و هو النوع الأكثر شيوعاً لبساطته.

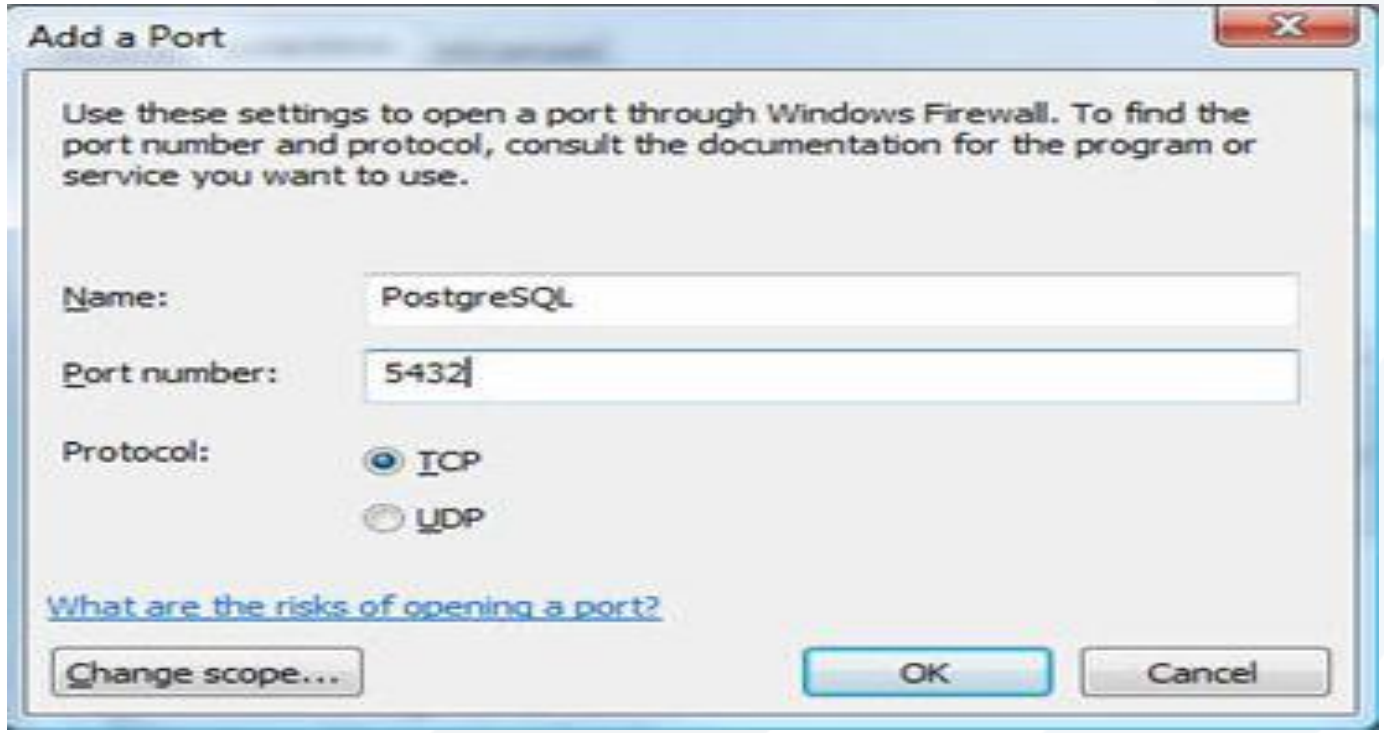
الجدران النارية (5/5)

(Firewalls)

❖ يوجد نوعان للجدران النارية:

2. النوع الثاني: يعتمد على **أرقام المنافذ** ليحدد فيما إذا كنت تريد السماح بالاتصال عبر هذا المنفذ أم لا.

هذا النوع أقل شيوعاً و ذلك بسبب تعقيده.



جَامعة
المَنارة
MANARA UNIVERSITY

Thanks

The end