جامعة المنارة

كلية الهندسة

قسم المعلوماتية

أمن 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
- ما الفرق بين مفهومي أمن المعلومات و الأمن السيبراني؟
- 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		شبكة
اتصالات مغلقة (Closed Communication)	⟵ ⟶	اتصالات مفتوحة (Open Communication)
وصول مقيد Full Lockdown	⟵ ⟶	وصول كامل Full Access

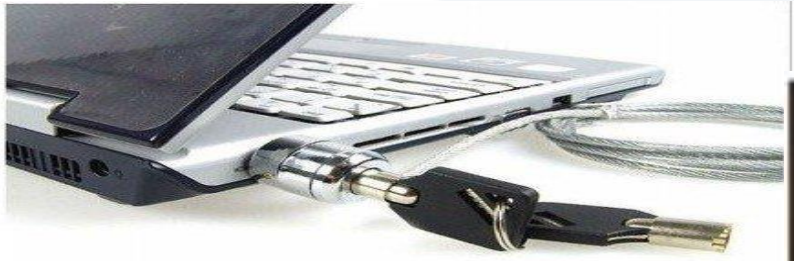
يجب تحقيق التوازن بين المفهومين

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..

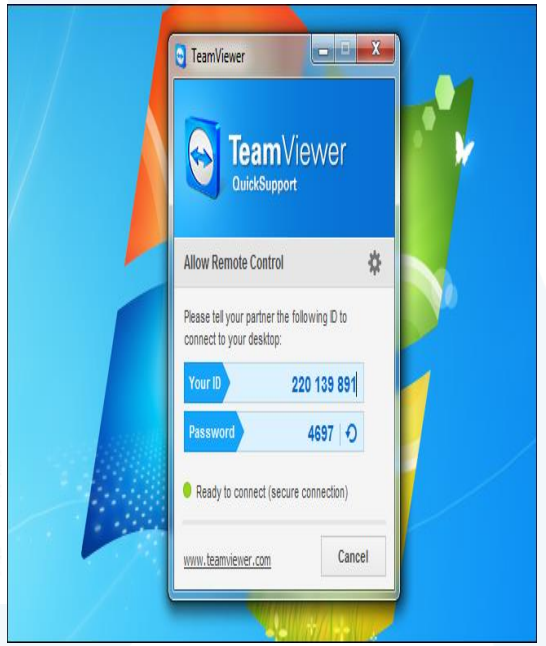


أنواع التحكم بأمن المعلومات (2/3)

- 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)

المَـنارة
MANARA UNIVERSITY

✓ 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 الانترنتIPTV، 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 ...

التوافرية
(Availability)

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

المصادقة
Authentication

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

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

- مثال1: سرقة نسخة من ملف غير مشفر
  - الموثوقية Confidentiality: غير محققة لأن الملف لم يعد سرياً
  - التكاملية Integrity: محققة لأنه لم تُجر أية عملية تعديل
  - التو افرية Availability: محققة لأن الملف لا يزال متاح ويستطيع المستخدمون الوصول إليه
- مثال2: إرسال ملف مشفر فيه معلومات مزيفة
  - الموثوقية Confidentiality: محققة لأن الملف بقي سرياً
  - التكاملية Integrity: غير محققة لأنه حُشرت 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

  - الموثوقية Confidentiality: محققة لأن الملف بقي سرياً
  - التكاملية Integrity: محققة لأنه لم تُجرَ أية عملية تعديل
  - التو افرية Availability: غير محققة لأن الملف لم يعد متاحاً

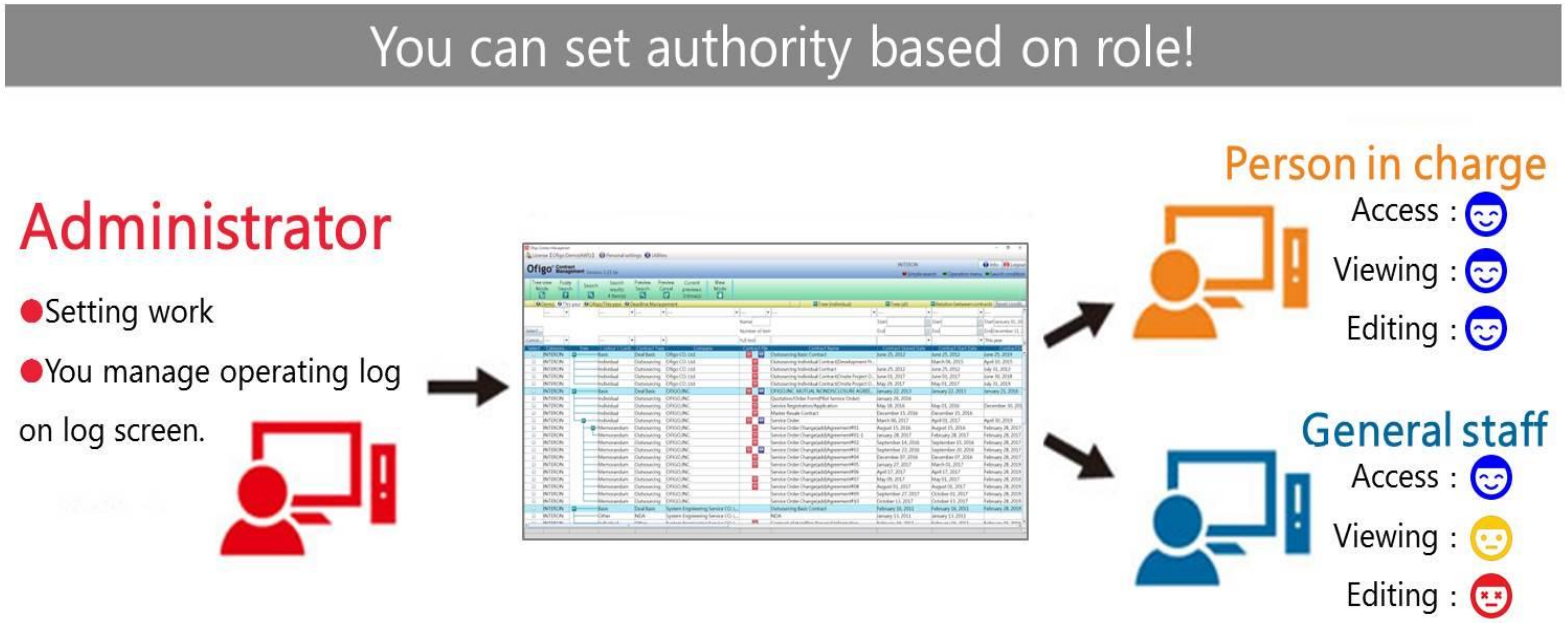
التحكم بالوصول
(Access Control)

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

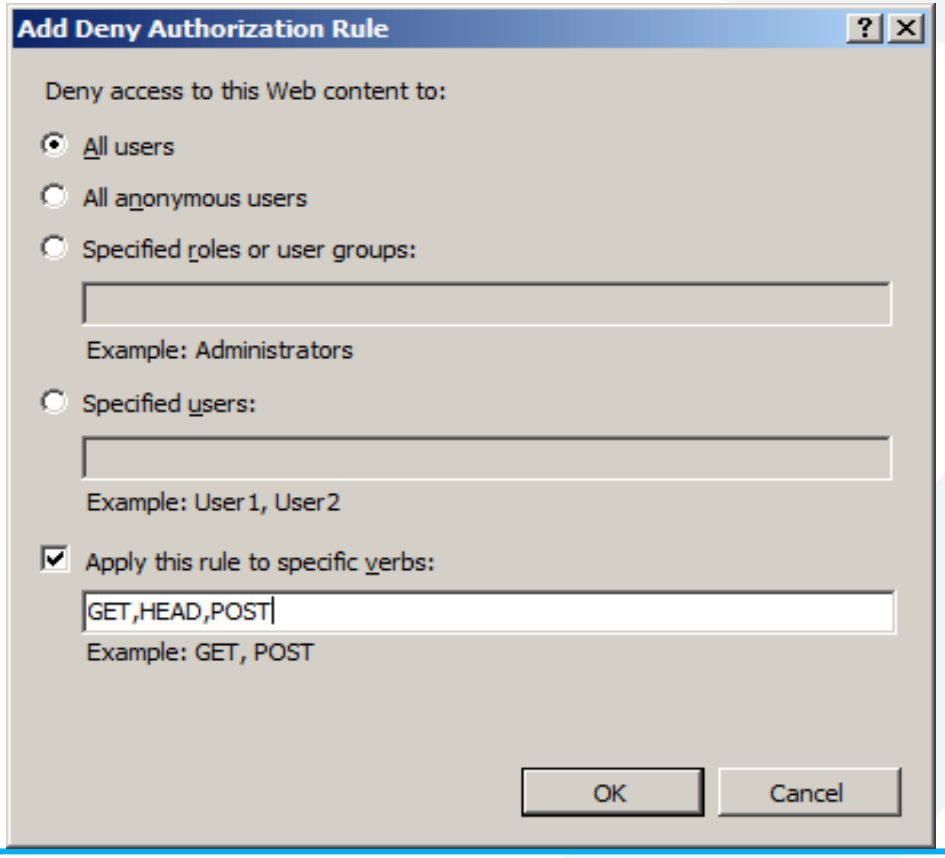
إنه أسلوب ينظم **مَنْ وماذا يمكن عرضه أو استخدامه من الموارد في نظام ما**

أي : تحدد مستوى الوصول المسموح به لكل مستخدم

- يرتبط غالباً بالمصادقة: فبعد أن تنفذ عملية المصادقة يحدد النظام ما هو مسموح به، وبذلك يتجنب النظام المستخدمين غير المخول لهم الوصول إلى البيانات.

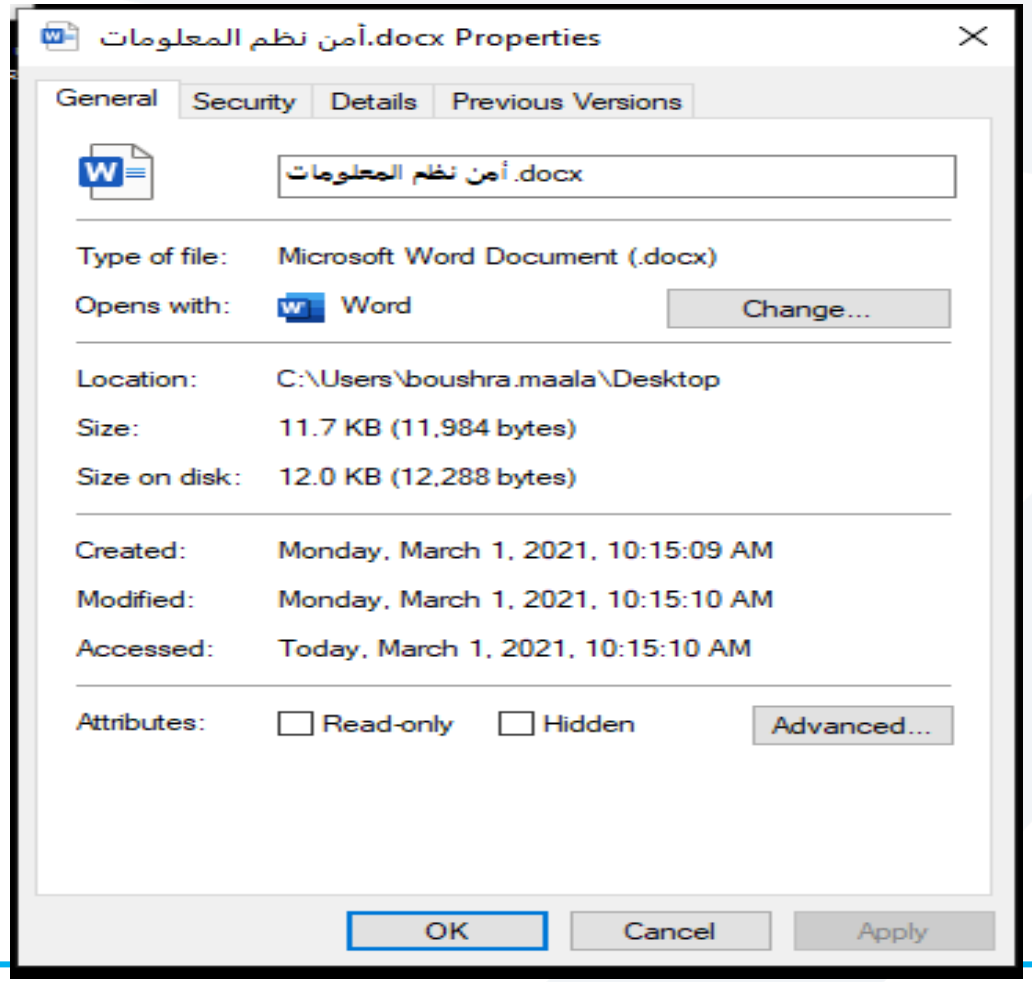


الترخيص/ التفويض
(Authorization)



- ✓ 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.

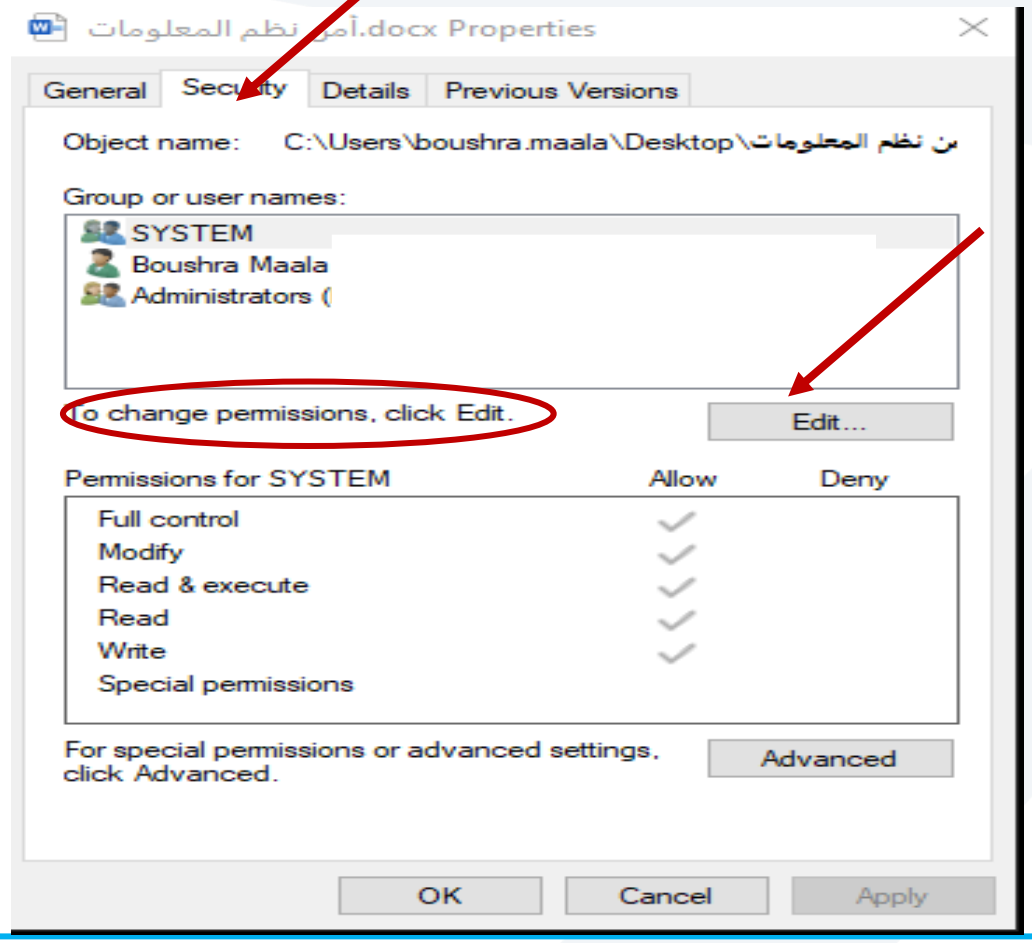
مثال عن التفويض (Authorization) في ملف وورد



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

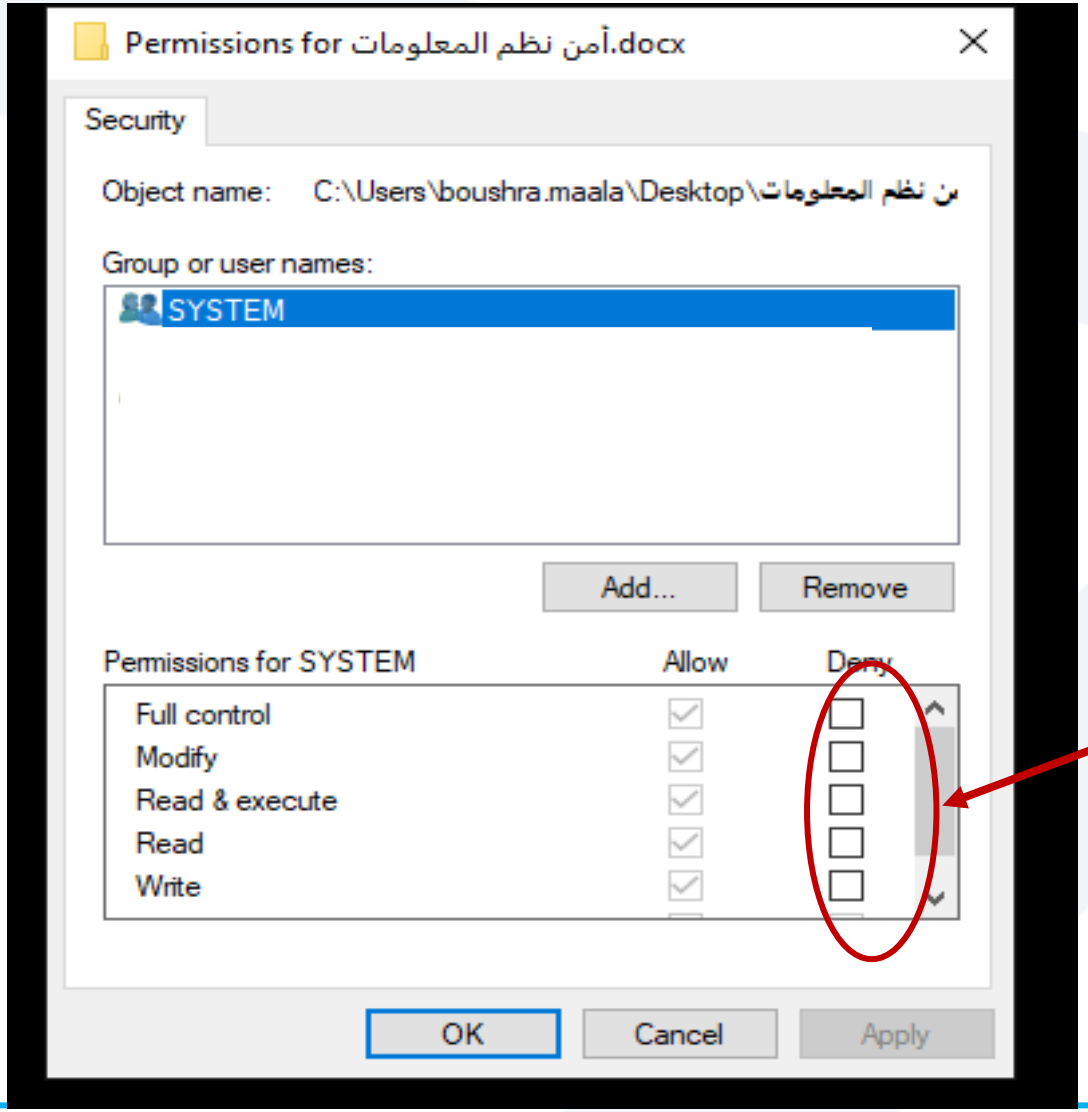
مثال عن التفويض (Authorization) في ملف وورد

نختار security ✓



نختار تغيير التفويض ✓

مثال عن التفويض (Authorization) في ملف وورد



من هنا يمكن أن نضع السماحيات التي نريدها

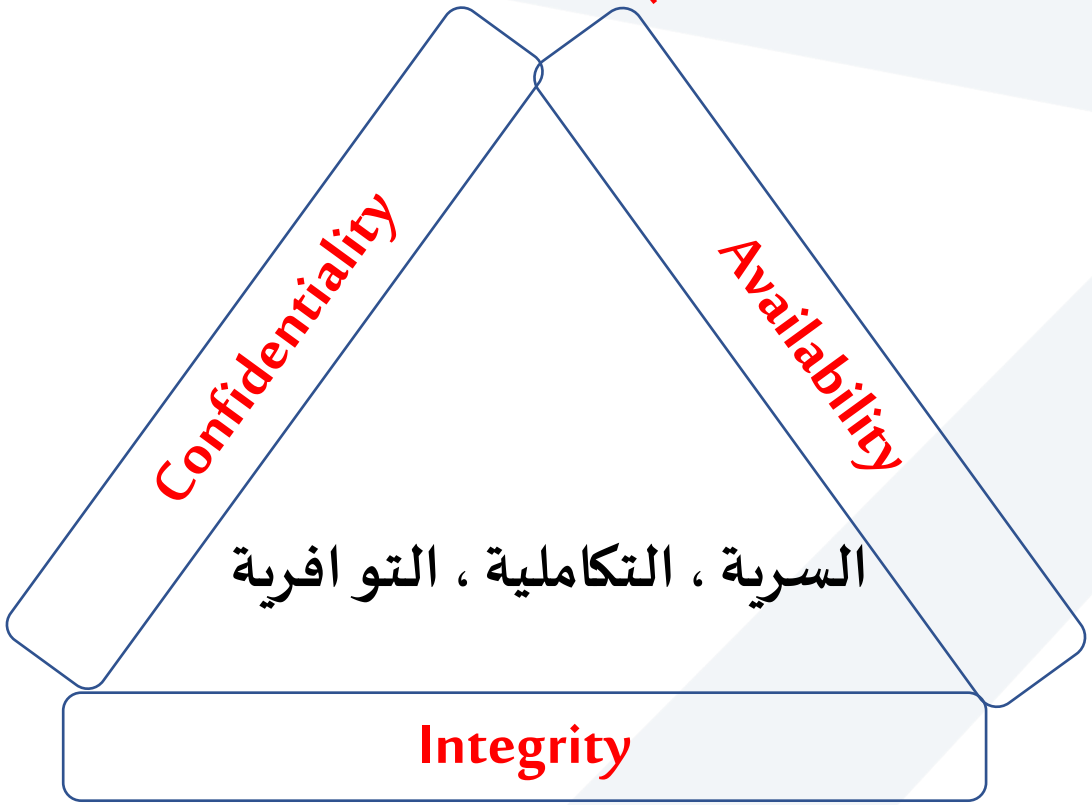
عدم التنصل
(Non-Repudiation)

- ✓ 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.

المثلث الأمني CIA

(Confidentiality, Integrity, Availability)

يمكننا أن نقول أن المعلومات آمنة إذا تحقق المثلث الأمني



ما الفرق بين مفهومي أمن المعلومات و الأمن السيبراني؟

- يختلفان عن بعضهما من حيث الهدف و المجال المطبق ضمنه ، لكن غالباً ما يستخدم المصطلحان لطرح نفس الفكرة .

الأمن السيبراني (Cybersecurity) هو فئة من أمن المعلومات

- **يغطي أمن المعلومات:**
  - ✓ الأمن الفيزيائي
  - ✓ أمن الطرفيات
  - ✓ تشفير البيانات
  - ✓ أمن الشبكات
  - ✓ الحماية من كل التهديدات

- **يختص الأمن السيبراني :**

منع أو تخفيف الهجمات المتعلقة بالتقنيات (كالفيروسات ، البرامج الخبيثة ..)

الهجمات ضد الأمن (1/4)

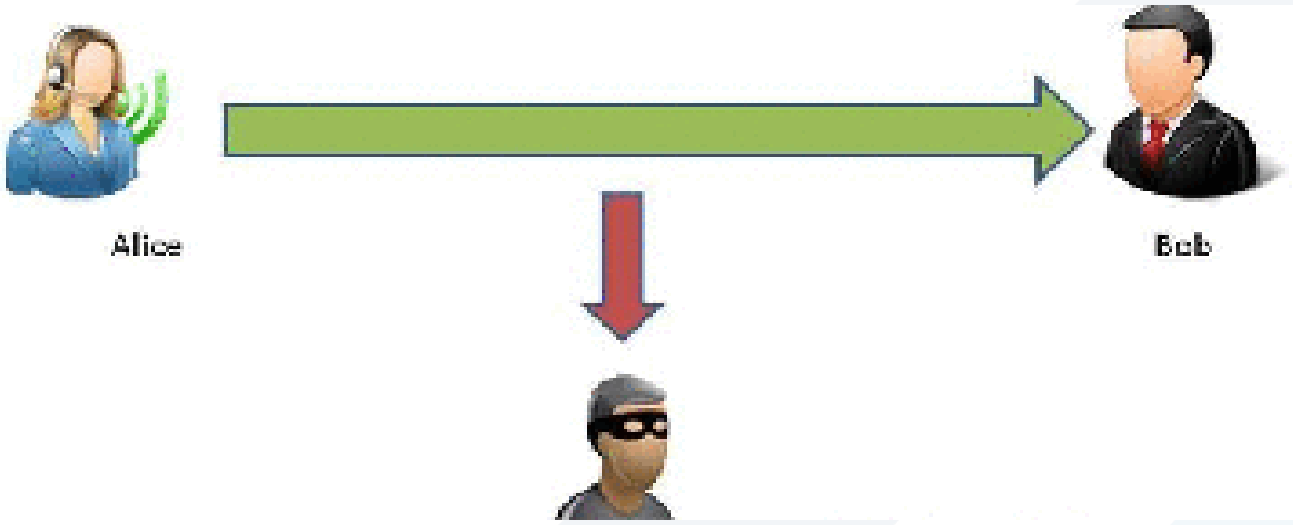
- **الهجوم** هو الاعتداء على أمن النظام ، هذا الهجوم قد يكون بـ:

1. **الاعتراض (Interception):**

✓ أن يستطيع المهاجم الوصول إلى جزء من مكونات النظام غير مسموح له الوصول إليه.

✓ مثلاً هجوم التنصت على الاتصال اللاسلكي

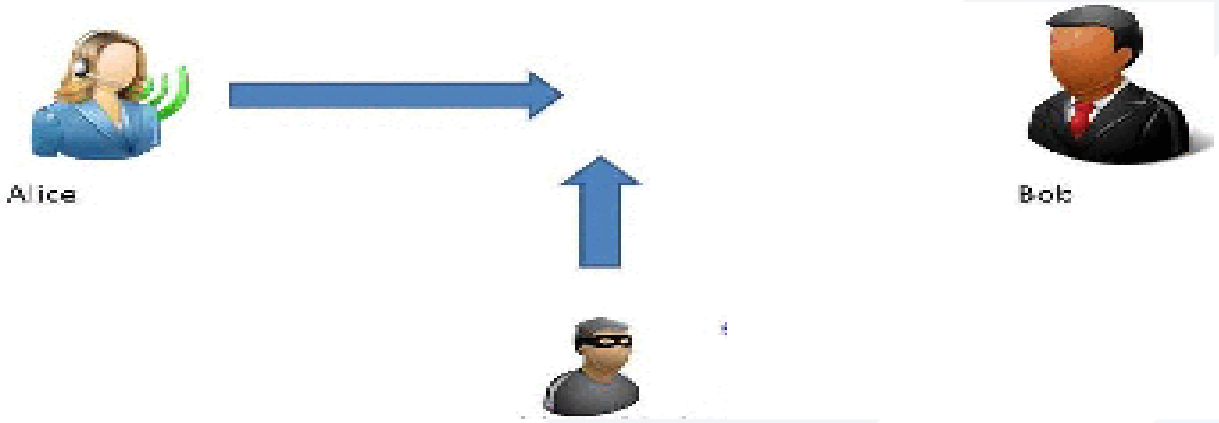
✓ يهدد الموثوقية (Confidentiality)



الهجمات ضد الأمن (2/4)

2. الانقطاع (Interruption):

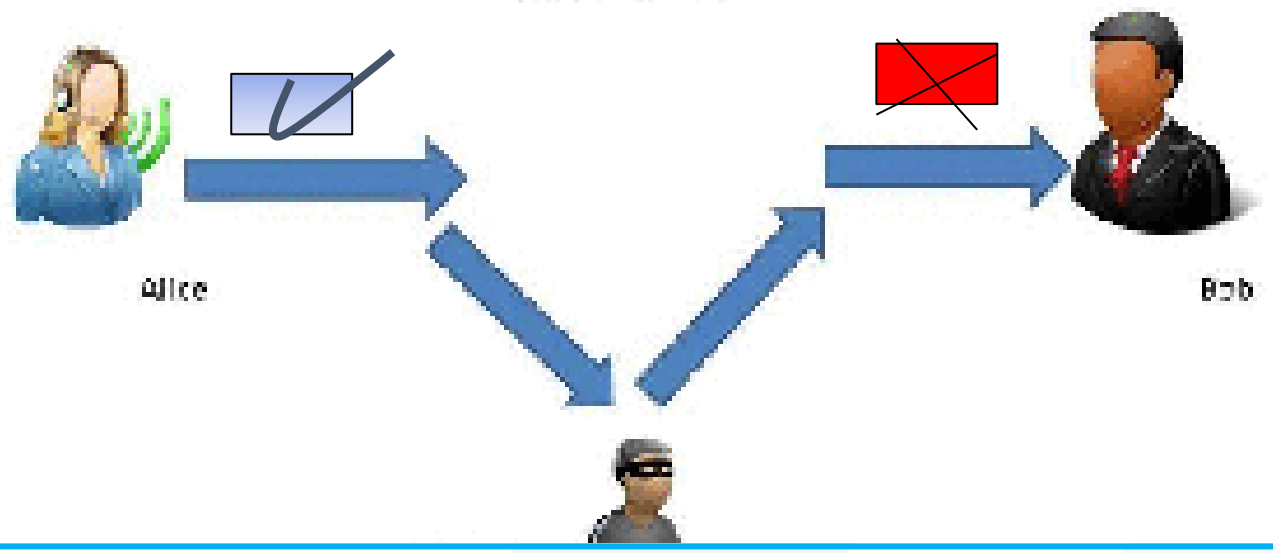
- ✓ أن يدمر المهاجم أحد مكونات النظام بحيث يصبح غير متوفر أو خارج الخدمة .
- ✓ مثلاً قطع الاتصال السلكي ، التشويش على الاتصال اللاسلكي ، إسقاط الرزم.
- ✓ يهدد التوافرية (Availability)



الهجمات ضد الأمن (3/4)

3. التعديل (Modification):

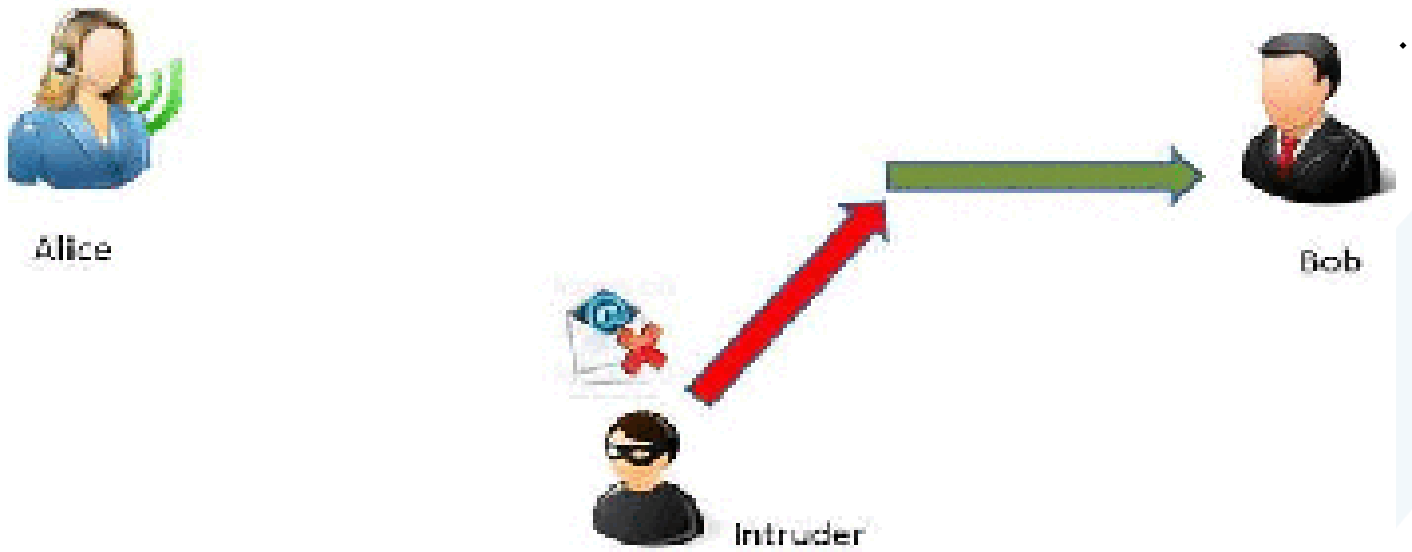
- ✓ أن يستطيع المهاجم الوصول إلى جزء من مكونات النظام غير مسموح له الوصول إليه ويعبث بهذا الجزء.
- ✓ يهدد تكاملية المعلومات (Data integrity)



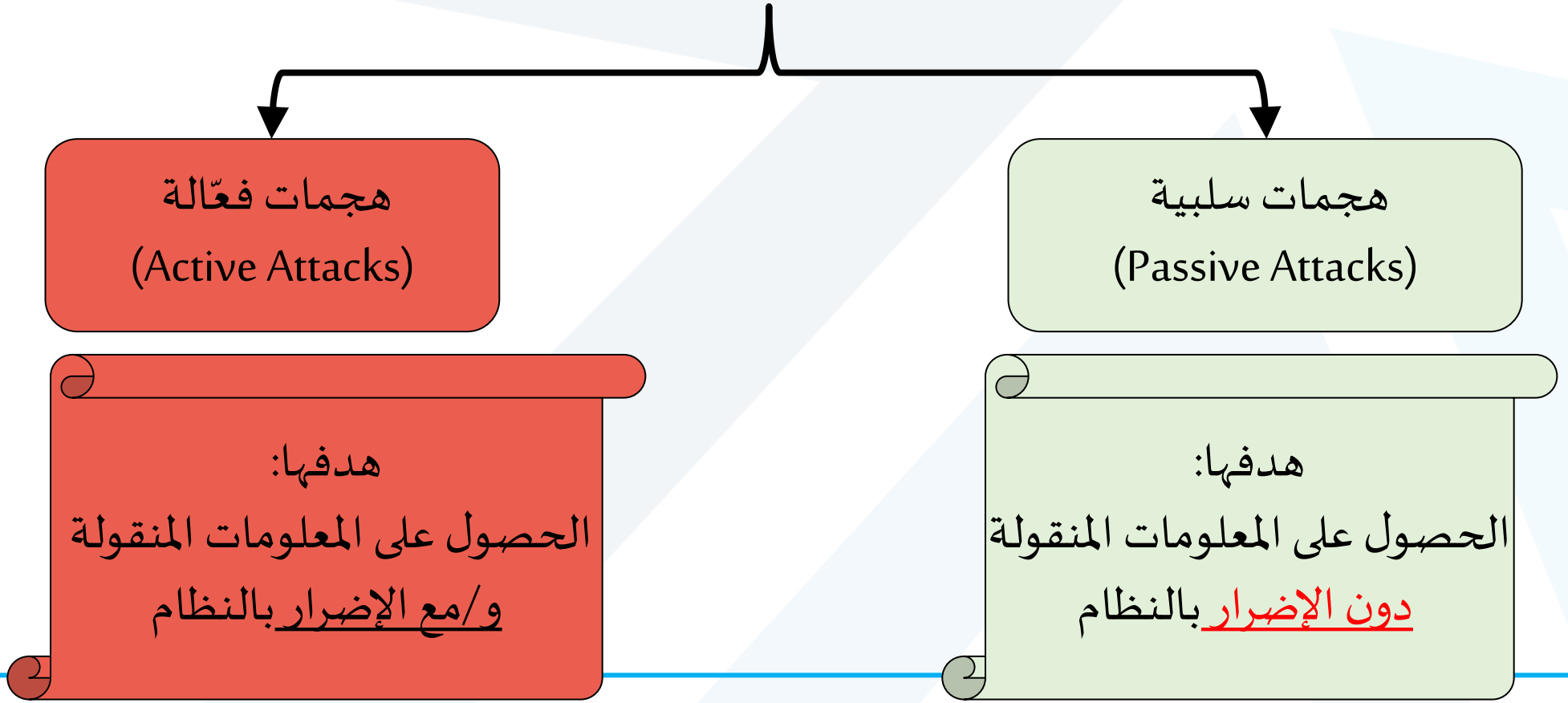
الهجمات ضد الأمن (4/4)

4. التزييف (Fabrication):

- ✓ أن يحشر المهاجم معلومات مزيفة (أهداف مزيفة) ضمن النظام.
- ✓ مثلاً هجوم تزييف العنوان (IP Spoofing) .
- ✓ يهدد المصادقة (Authentication)



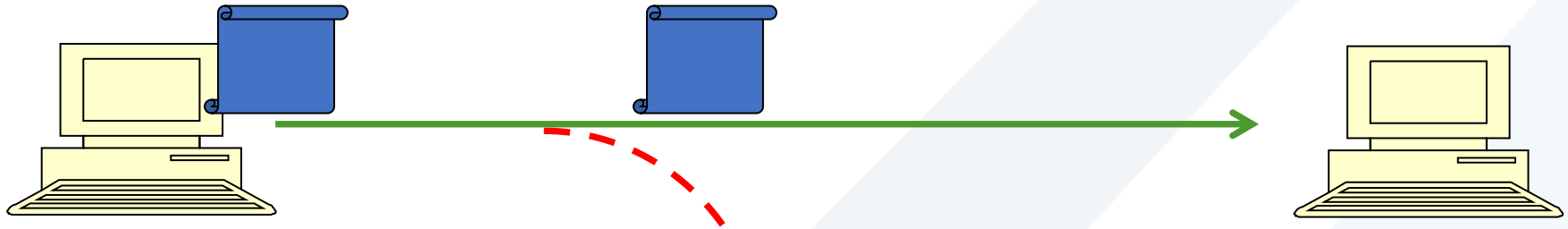
تصنيف كنت للهجمات ضد الأمن
Kent's classification



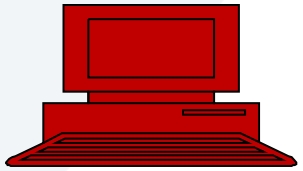
الهجمات السلبية (1/2)

- هي الهجمات التي تتضمن عملية التنصت و مراقبة الإرسال
  - ✓يوجد نوعان:

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

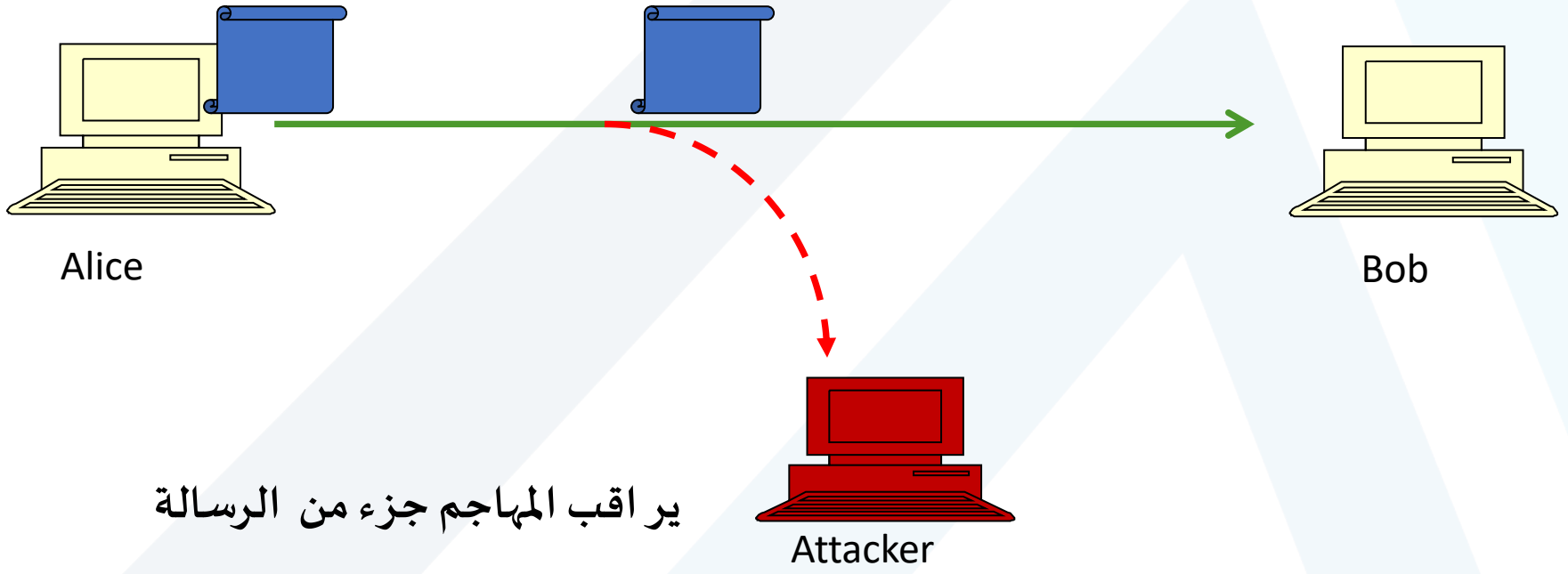


يقرأ المهاجم محتوى الرسالة



الهجمات السلبية (2/2)

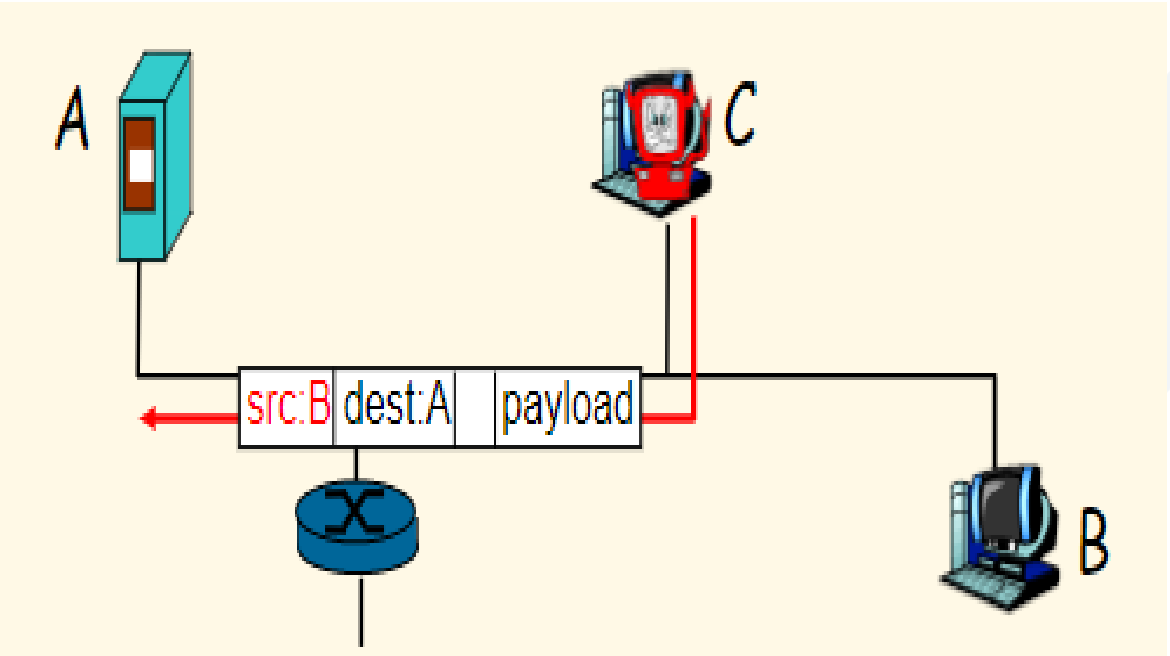
2. تحليل حركة المعلومات (Traffic analysis)



الهجمات الفعالة (1/4)

- ❖ 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)

مهاجم

زبون

Bob@yourcompany.com

المسؤول المالي

Alice@yourcompany.com

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

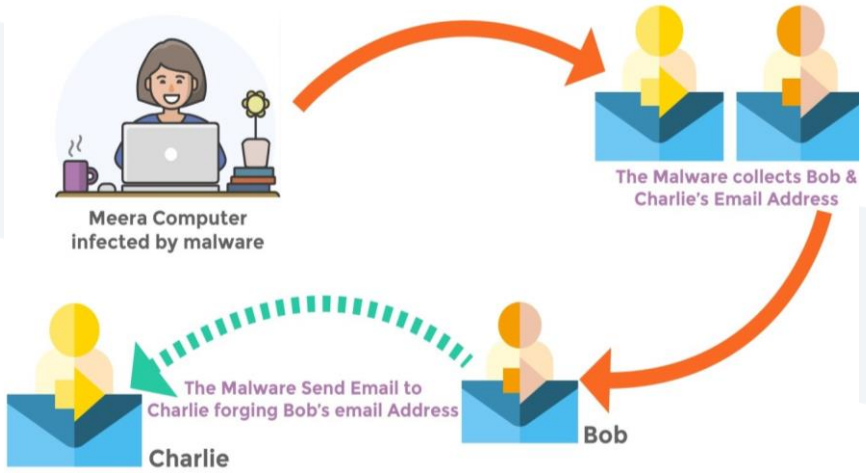
يترتب عليك تحويل مبلغ 50000 $ إلى الحساب الآتي 1211212قبل نهاية اليوم أو تتوقف جميع المعاملات التجارية الجارية حاليا لصالحك.

سيفترض Bob أن الإيميل شرعي وسيجري التحويل

زبون

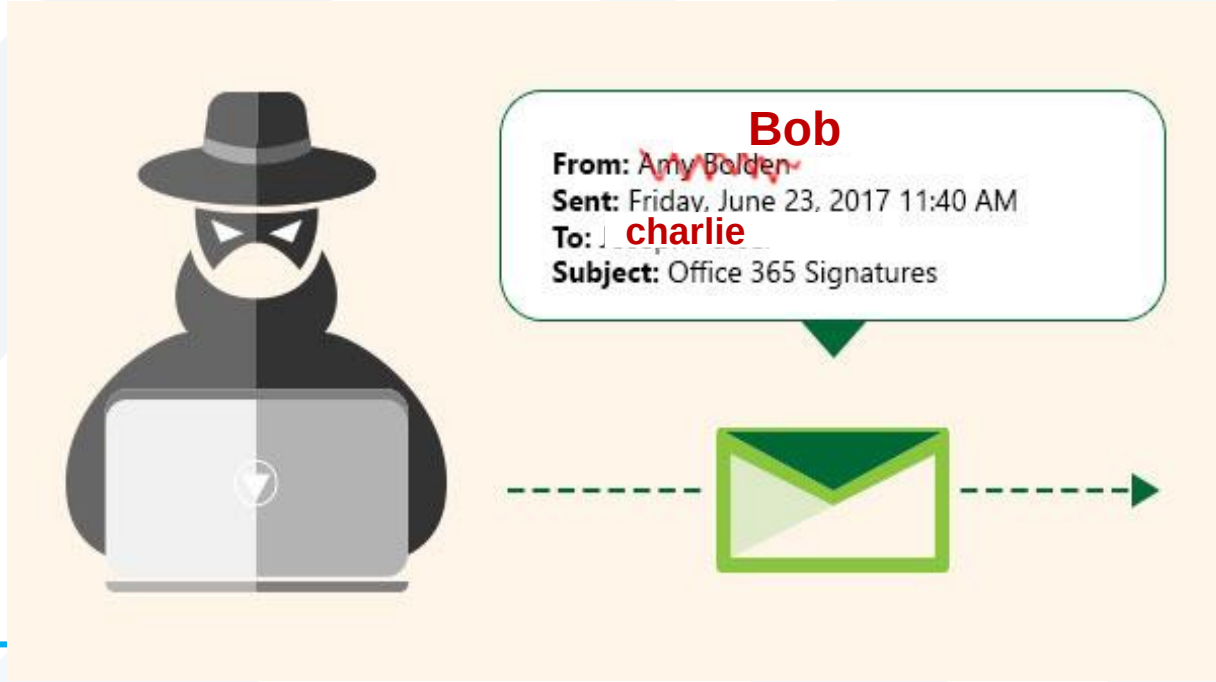
مهاجم

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



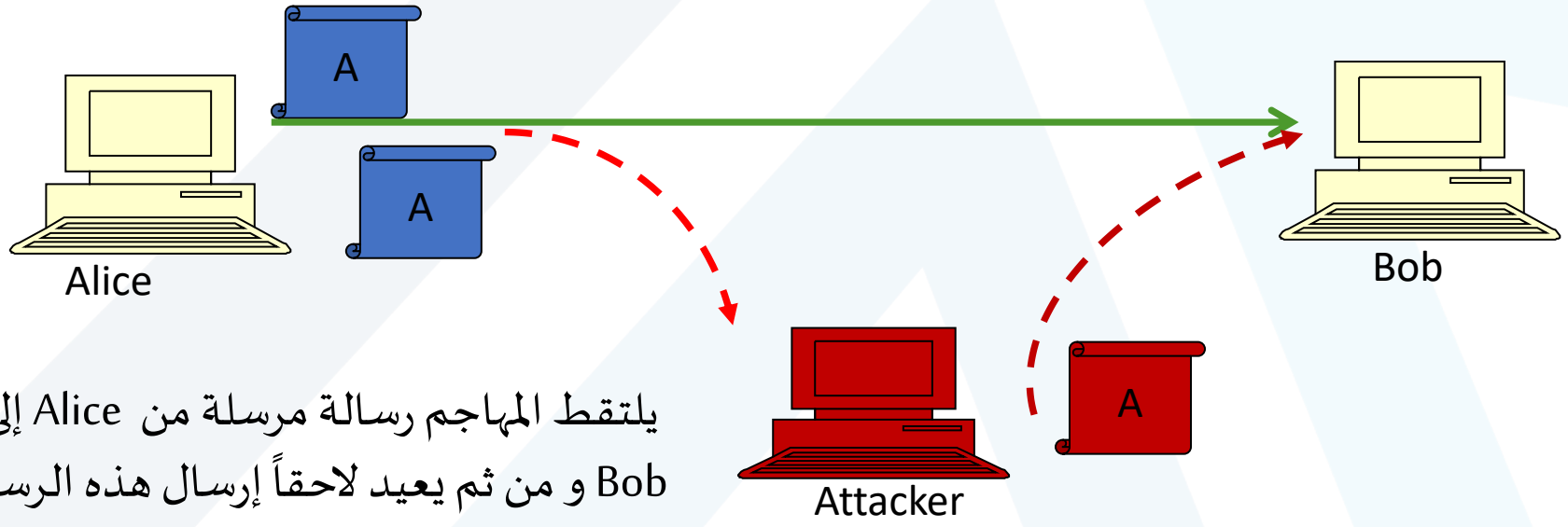
- هذه الطريقة بالهجوم أعقد من المثال السابق
- هناك برامج تسمح للمهاجم أن يضع في جهة المرسل العنوان الذي يريده وليس بالضرورة العنوان الذي يُرسَل منه بشكل فعلي.

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



الهجمات الفعالة (2/4)

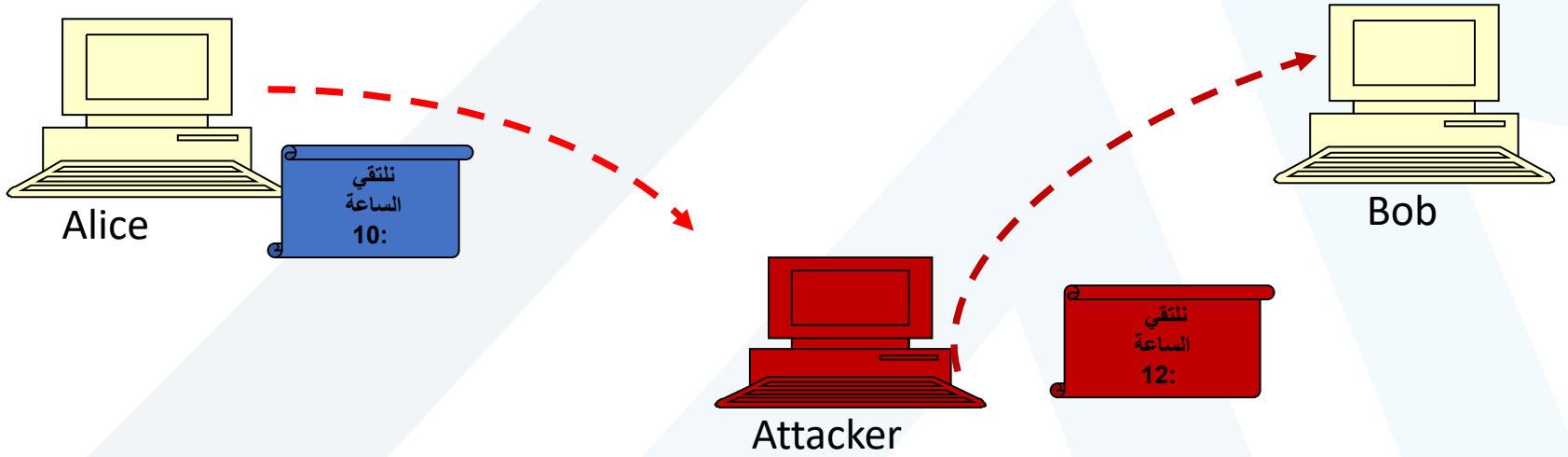
2. إعادة الإرسال (Replay Attack)



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

الهجمات الفعالة (3/4)

3. تعديل الرسائل (Modification of message)



يعدل المهاجم رسالة مرسلة من Alice إلى Bob

الهجمات الفعالة (4/4)

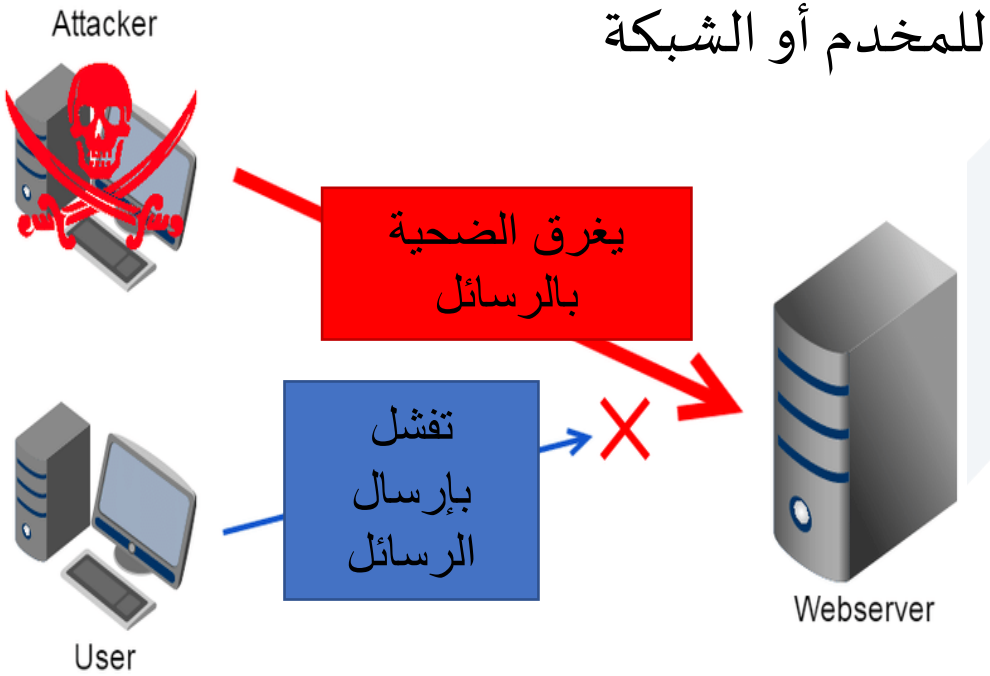
4. حجب الخدمة DoS (Denial of Service)

هدفه:

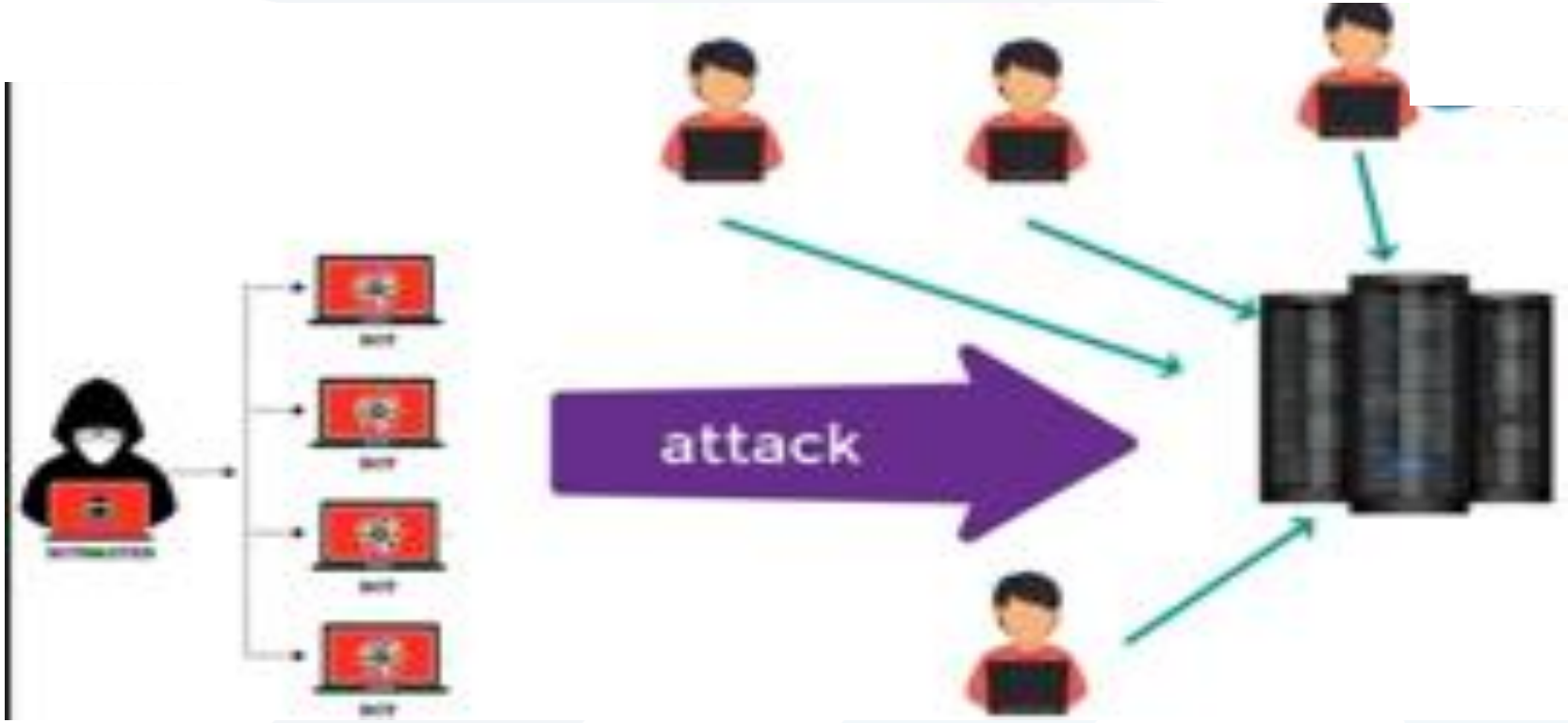
جعل الخدمة غير متوفرة من خلال التحميل الزائد(overloading) للمخدم أو الشبكة

من خلال:

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

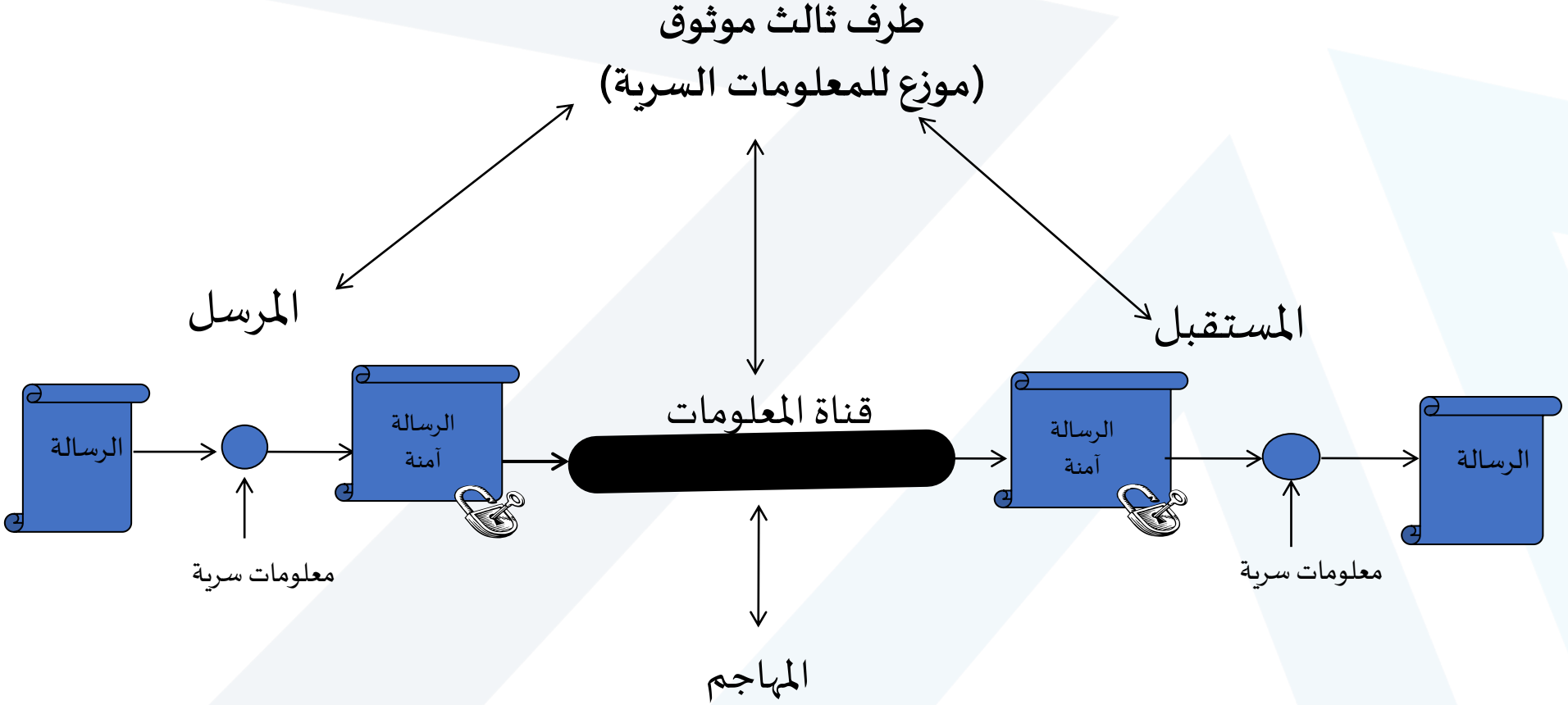


الهجمات الفعالة (4/4)



حجب الخدمة الموزع DDoS (Distributed Denial of Service)

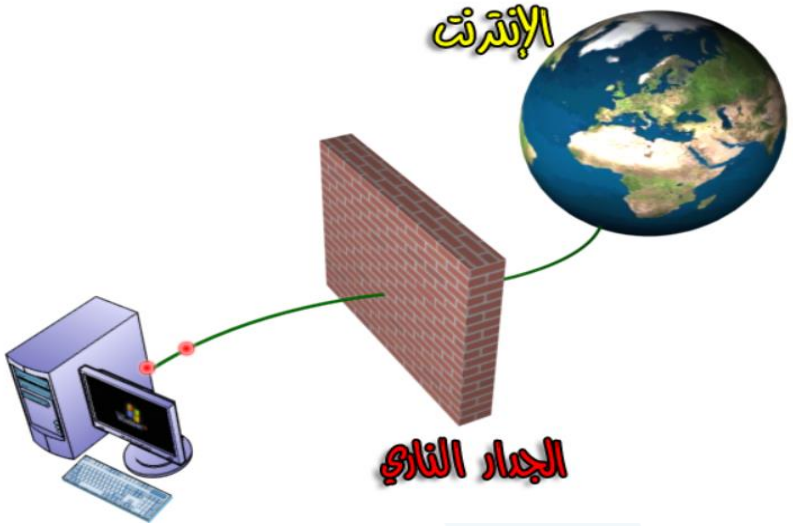
نموذج أمن الشبكة
(Security Network Model)

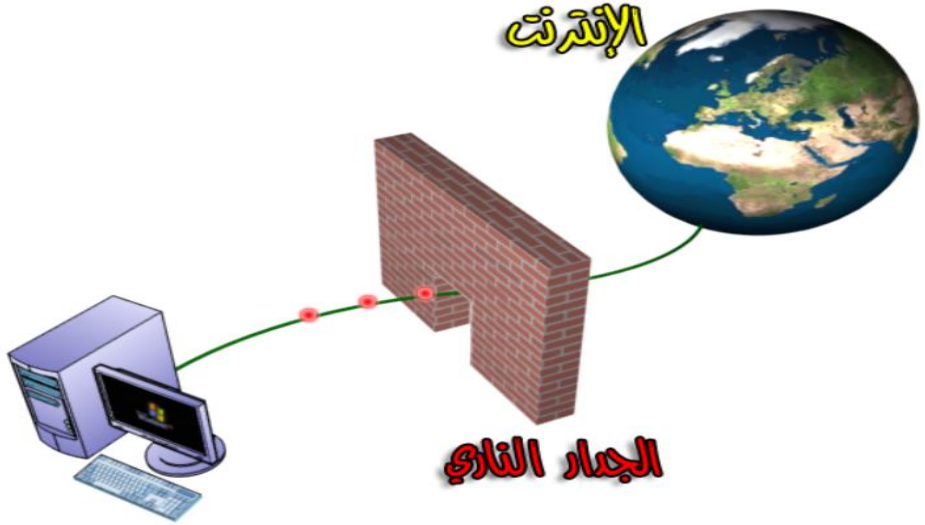


الجدران النارية (الحماية) (1/5)

(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 (الحماية) (2/5)

(Firewalls)

❖ تكون الجدران النارية إما :

➢ برمجيات (Software)

(Host-based firewall)

- هي الأرخص والأكثر انتشاراً
- سهلة التنزيل عادة تكون موجودة افتراضياً مع نظام windows .
- خاصة بحماية جهاز واحد فقط.
- لكنها قد تستهلك جزء اً كبيراً من موارد النظام
- وقد تتسبب في مشاكل مع برمجيات أخرى موجودة على الجهاز

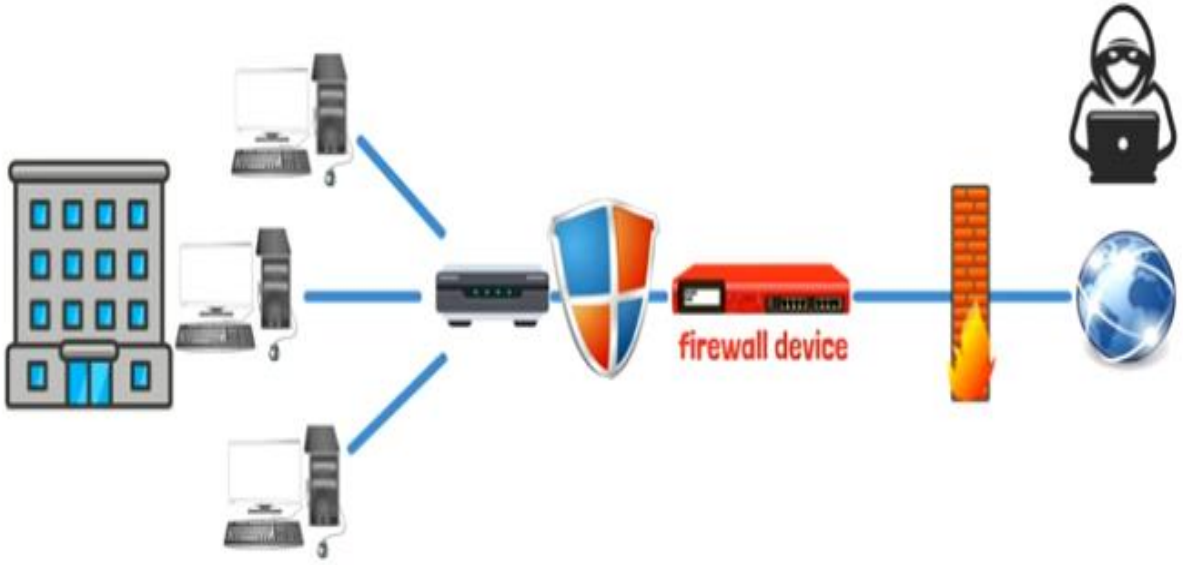
الجدران النارية (الحماية) (3/5)

(Firewalls)

❖ تكون الجدران النارية إما :

✓عتاد صلب (Hardware)

- يستخدم بشكل أكبر في الشركات والمؤسسات الكبيرة
- هو جهاز فيزيائي يوضع بين الموجهات وشبكة الانترنت



الجدران النارية (الحماية) (3/5)

(Firewalls)

❖ تكون الجدران النارية إما :

✓عتاد صلب (Hardware)

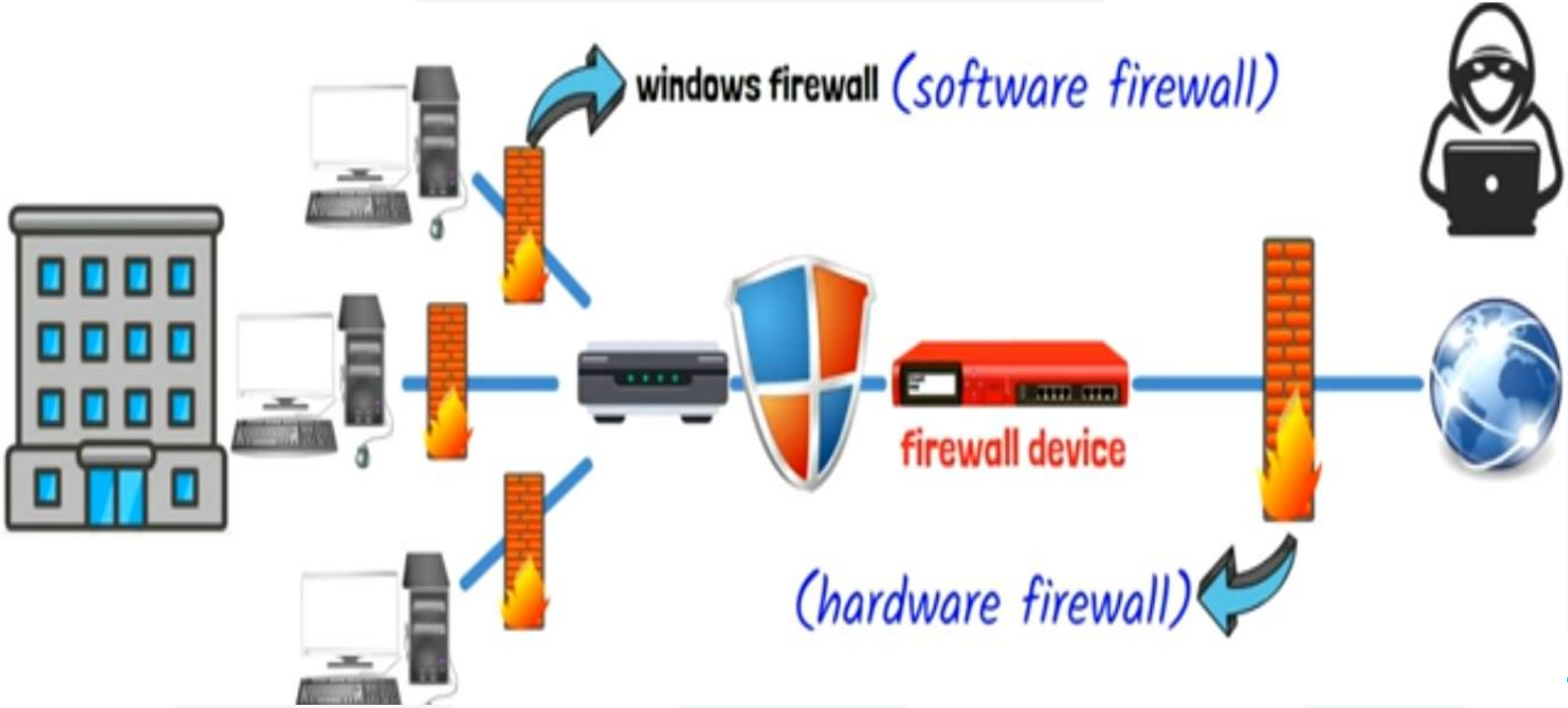
- هي مخصصة من أجل تطبيق وظائف الجدران النارية لذا لا تستهلك من موارد الأجهزة الحاسوبية
- عيبها الأساسي هو الصيانة وذلك لصعوبة تهيئتها وتحديثها بشكل صحيح

الجدران النارية (الحماية) (3/5)

(Firewalls)

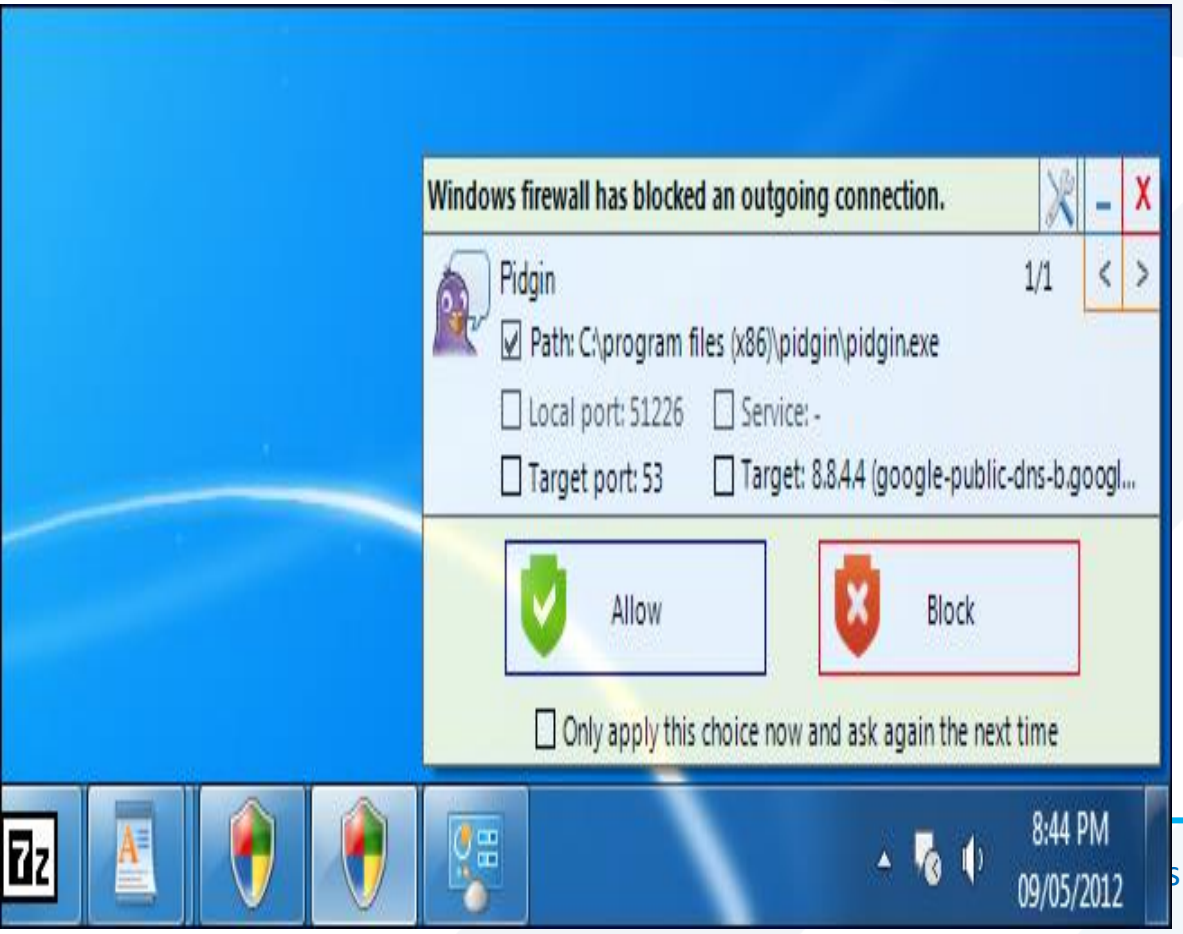
- عادة ما يستخدم النوعان السابقان معاً و هذا ما يتنج عنه ما يسمى بـ

Network –based firewall



الجدران النارية (4/5)

(Firewalls)



❖ يوجد نوعان للجدران النارية حسب آلية عمله:

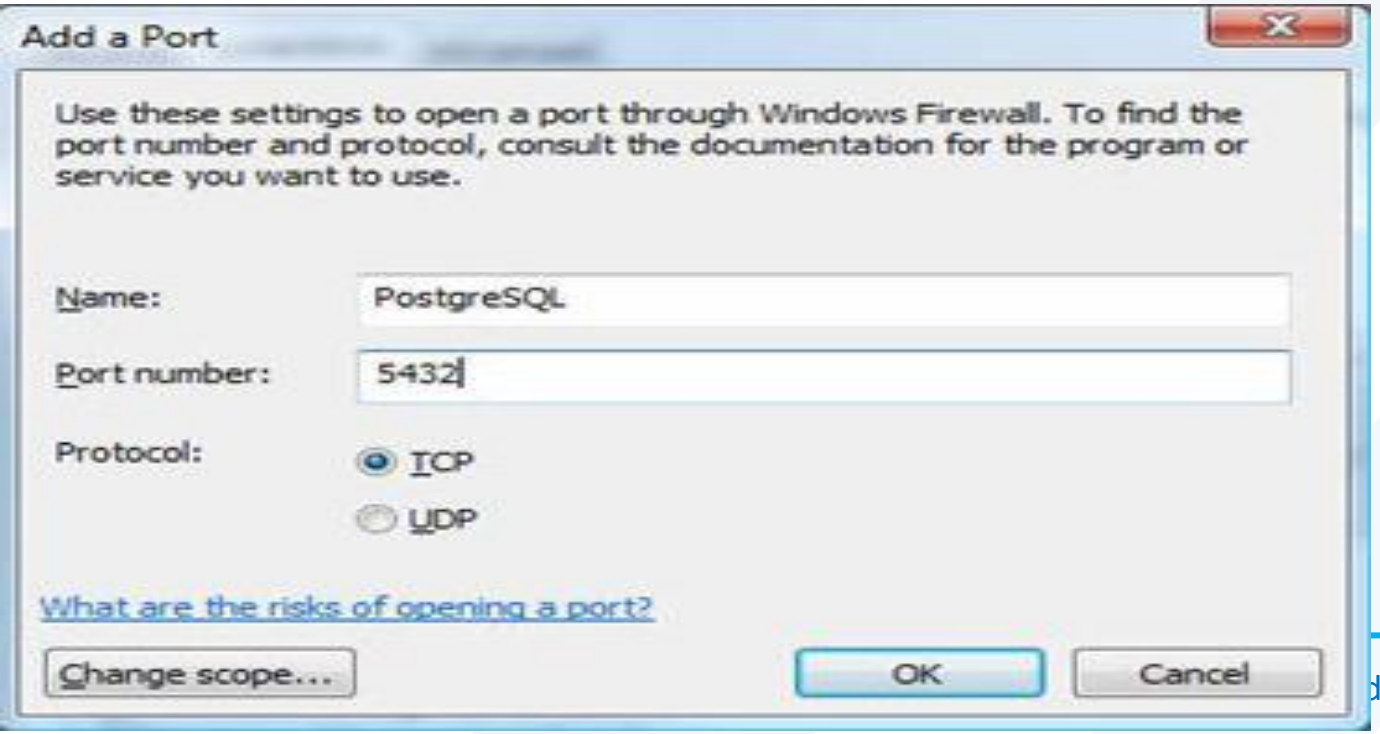
1. النوع الأول : يعتمد على **أسماء البرامج** لتحديد فيما إذا كانت مسموح لها الاتصال بالانترنت أم لا. و هو النوع الأكثر شيوعاً لبساطته.

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

فيديو توضيحي للجدران النارية

جَامعة المَنارة
MANARA UNIVERSITY

نهاية المحاضرة الأولى