Attacks أنواع الهجوم

يقسم الهجوم إلى أربعة أقسام وهي:

1- Interception Attacks: هجوم التصنت على الرسائل

وفكره عمل هذا الهجوم :أن المهاجم يراقب الاتصال بين المرسل والمستقبل للحصول على المعلومات السرية وهو ما يسمى بالتصنت على الاتصال.

2- Interruption Attacks: هجوم الإيقاف

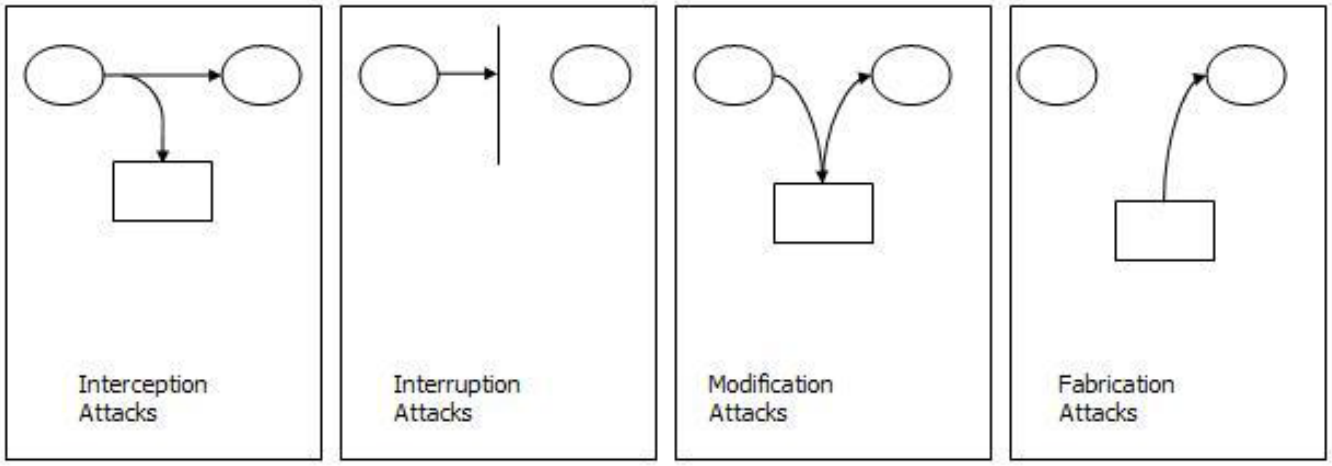
وهذا النوع يعتمد على قطع قناة الاتصال لإيقاف الرسالة أو البيانات من الوصول إلى المستقبل وهو ما يسمى أيضا برفض الخدمة

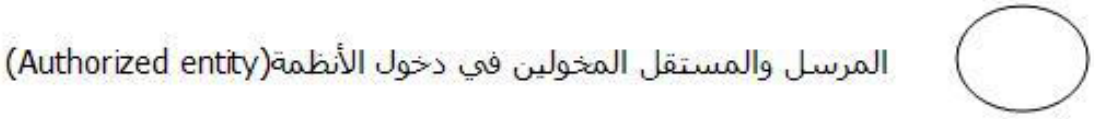
3 - هجوم يعدل على محتوى الرسالة

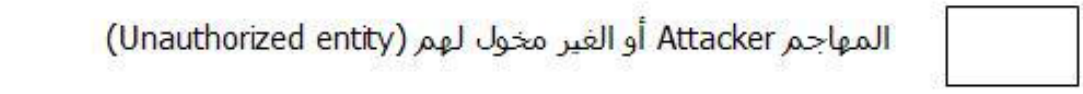
فإنه Attacker وهنا يتدخل المهاجم بين المرسل والمستقبل) يعتبر وسيط بين المرسل والمستقبل (وعندما تصل إلى ال
يقوم بتغيير محتوى الرسالة ومن ثم إرسالها إلى المستقبل ، والمستقبل طبعا لا يعلم بتعديل الرسالة من قبل ال.Attacker

4 - Fabrication Attacks: الهجوم المزور أو المفبرك

وهنا يرسل المهاجم رسالة مفادها انه صديقه ويطلب منه معلومات أو كلمات سرية خاصة بالشركة مثلا .







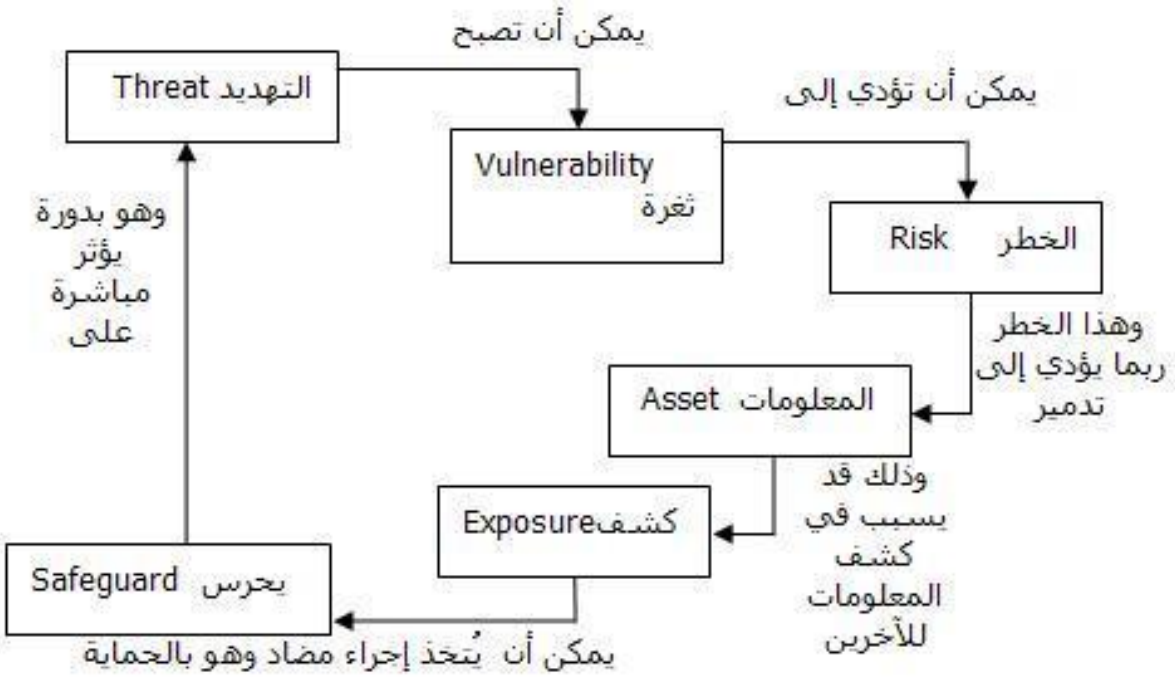
تعريف الخطر Risk وأقسامه:

الخطر Risk هو أنه يوجد على الأرجح تهديد يمكن إستغلاله ، وبالتالي إذا استغل ذلك التهديد يمكن أن نطلق عليهVulnerability أو ثغرة ، حيث أنه يوجد ثغرة أمنية في تلك المنظمة .
ومن هذا التعريف يمكن أن نقسم ال Risk إلى قسمين رئيسيين هما:

- التهديد (Threat): وهو عملية المحاوله الى الوصول إلى المعلومات السرية الخاصة بالمنظمة

• (Vulnerabilities) الثغرات وهي أنه يوجد ضعف في المنظمة يستطيع المهاجم Attacker الدخول من خلالها.

وهناك مكونات أخرى لل Risk وهي كما يوضح الشكل التالي:



التشفير Encryption

علم التشفير : Cryptography كلمة يونانية الأصل kryptós تعني مخفي و gráphien تعني كتابة الكتابة المخفية.

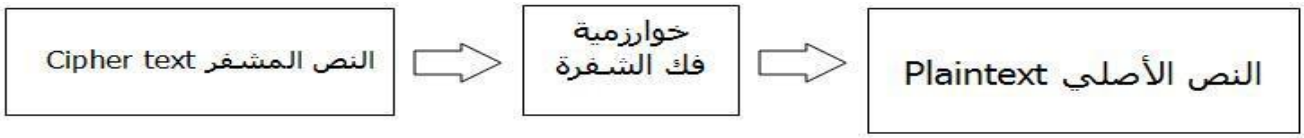
تعريف علم التشفير :
هو علم يهدف إلى حماية المعلومات (سر معين) فإذا كان لدي نظامين يتشاركان سر معين يستخدمان التشفير لحماية سريته ويمكن تحقيق خدمات أخرى من التشفير مثل التحقق من مصدر الرسالة.

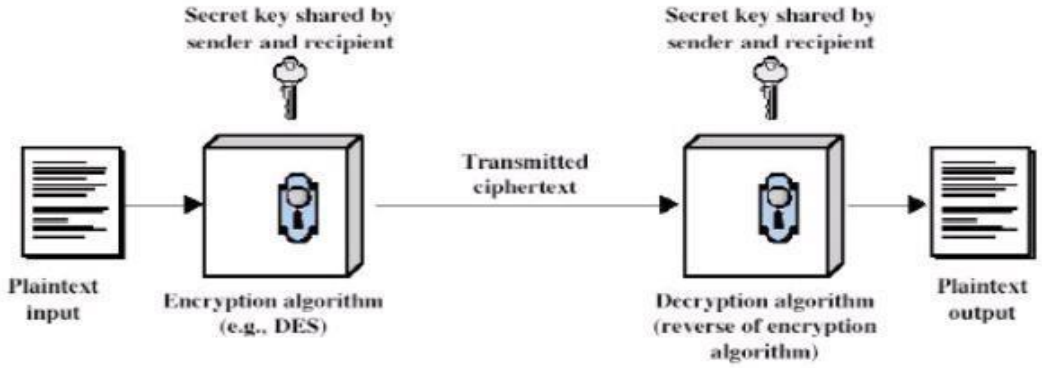
التشفير استخدم قديما في الحضارات القديمة لإخفاء المعلومات والمراسلات مثل الحضارة الفرعونية والدولة الرومانية .ولكن التشفير كعلم مؤسس منظم يدين بولادته ونشأته للعلماء الرياضيين واللغويين العرب إبان العصر الذهبي للحضارة العربية ومن أشهرهم الفراهيدي والكندي، وقد ألف هؤلاء العلماء مفاهيم رياضية متقدمة من أهمها التوافيق والتباديل . وكذلك توظيف الكندي ومن تبعه مفاهيم الإحصاء والاحتمالات في كسر الشفرة
وقد شاع في أيامنا استخدام مصطلح" التشفير "ليدل على إخفاء المعلومات .ولكن كلمة" التشفير "وافدة من اللغات الأوربية (Cipher) وهذه بدورها جاءت أصلا من اللغة العربية ولكن بمعنى آخر لكلمة" الصفر ." فكما هو معلوم أن العرب قد تبنوا مفهوم الصفر والخانات العشرية واستخدموه في الحساب، وهو ما لم يكن الأوربيون يعرفونه في القرون الوسطى ، وكان مفهوم الصفر جديدا وغريبا لدرجة أنهم أخذوه بنفسالاسم

فأسموه "Cipher ولأن مفهوم الصفر الجديد كان في منتهى التعقيد والغموض فقد صاروا يستخدمون كلمة Cipher للدلالة على الأشياء المبهمة وغير الواضحة.

التشفير :هو تحويل المعلومات المهمة أو التي لا تريد أن يطلع عليها أحد إلى نص مخفي أي لا يمكن فهمه

وعملية فك التشفير كالتالي:





مصطلحات :

النص الواضح : (Plaintext) الرسالة الأصلية.
النص المشفر :(Ciphertext) الرسالة المشفرة.
الشيفرة:(Cipher) خوارزمية لتحويل النص الواضح إلى نص مشفر.
المفتاح : (Key) معلومة تستخدم في الشيفرة وتكون معروفة فقط للمرسل والمستقبل.
التشفير:(encrypt) encipher تحويل النص الواضح إلى نص مشفر.
فك التشفير:(decrypt) decipher إعادة النص المشفر إلى نص واضح.
علم التشفير:(cryptography) دراسة مبادئ وطرائق التشفير.
كسر التشفير:(codebreaking) cryptanalysis دراسة مبادئ وطرائق فك تشفير النص المشفر دون معرفة المفتاح.

التشفير بالطرق الكلاسيكية Classical Cryptography

يتم تقسيم طرق التشفير الكلاسيكية إلى قسمين رئيسيين, وهما:

1 - التشفير عن طريق الإحلال أو الإزاحة. Substitution cipher
2 - التشفير عن طريق إعادة الترتيب أو التبادل بين الأحرف. Transposition cipher

1. التشفير عن طريق الإحلال أو الإزاحة Substitution Cipher:

هذا النوع من التشفير يعتمد على إحلال حرف جديد مكان حرف من النص الأصلي, فنكون حصلنا على نص مشفر. فمثلاً لو كان لدينا الحرف (أ) في النص الأصلي, نستبدله بالحرف (س) فنكون شفرنا الحرف (أ) بالحرف (س), وهكذا. يمكن تقسيم التشفير عن طريق الإحلال إلى نوعين:

1.الشفرة الأبجدية الأحادية.Monoalphabetic Cipher
2.الشفرة الأبجدية المتعددة. Polyaphabetic Cipher