منتدى تو عرب التعليمي

www.arabia2.com/vb

موقع توعرب التعليمي

www.arabia2.com/vb

رؤية VISION 2030

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation
الإدارة العامة للمناهج

أتقن
التدريب المجتمعي

التدريب المجتمعي

الحقيبة التدريبية

الأمن السيبراني

(بنين & بنات)

مقدمة

الحمد لله وحده والصلاة والسلام على من لا نبي بعده، محمد بن عبد الله وعلى آله وصحبه، وبعد:

من منطلق حرص المؤسسة العامة للتدريب التقني والمهني وتماشيا مع تحقيق رؤية التحول الوطني والمساهمة في الخدمة المجتمعية رأت أن تتقدم خدمات تدريبية بعض الحقائب التدريبية بشكل مُبسط في محتوى تدريبي تقديمه في دورات قصيرة لا تتجاوز ١٦ ساعة تدريب في الأسبوع، تُقدم لجميع شرائح المجتمع الراغبين في اكتساب مهارات في أحد التخصصات التي تهمهم في حياتهم اليومية.

وتتناول هذه الحقيبة التدريبية " **الأمن السيبراني** " لمتدربي برامج التدريب المجتمعي أُتقِن OTQEN موضوعات حيوية تتناول الثقافة المهنية واكتساب المهارات الأولية لهذا البرنامج التدريبي.

والإدارة العامة للمناهج وهي تضع بين يديك هذه الحقيبة التدريبية تأمل من الله عز وجلً أن تسهم بالشكل مباشر في تأصيل المهارات الضرورية اللازمة، بأسلوب مبسط يخلو من التعقيد، مدعم بالتطبيقات والأشكال التي تدعم عملية اكتساب هذه المهارات.

والله نسأل أن يوفق القائمين على إعدادها والمستفيدين منها لما يحبه ويرضاه، إنه سميع مجيب الدعاء.

الإدارة العامة للمناهج

الفهــرس

تمهيد

الهدف العام من الحقيبة :

يهدف هذا البرنامج إلى إكساب المتدرب المهارات والمعلومات الأساسية في الأمن السيبراني.

تعريف بالحقيبة :

تقدم هذه الحقيبة المفاهيم الأولية الأساسية عن الامن السيبراني، حيث سيتمكن المتدرب من التعرف على الأمن السيبراني، ما المقصود بالتشفير ، الكتابة المخفية، تصميم الأكواد (التشفير)، بالإضافة إلى فك الأكواد (تحليل الشفرات).

الوقت المتوقع لإتمام التدريب على مهارات هذه الحقيبة التدريبية :

يتم التدريب على مهارات هذه الحقيبة في ١٦ ساعة تدريبية، موزعة كالتالي:

الوحدة ١ :	نظرية الأمن الإلكتروني	٤ ساعات تدريبية
الوحدة ٢ :	الأكواد الضارة	٤ ساعات تدريبية
الوحدة ٣ :	تأمين الشبكة	٤ ساعات تدريبية
الوحدة ٤ :	علم التشفير	٤ ساعات تدريبية

الأهداف التفصيلية للحقيبة :

من المتوقع في نهاية هذه الحقيبة التدريبية أن يتقن المتدرب ما يلي:

١ . التعرف على بيئة عمل الحاسوب الشخصي المعاصر.
٢ . التعرف على تخزين كلمة السر.
٣ . التعرف على تقنيات الهندسة الاجتماعية.
٤ . التعرف على عمليات الغش وكيفية تميزها.
٥ . كيفية تجنب أن تكون ضحية هجمات على شبكة الانترنت.
٦ . التعرف على الفيروسات وأخطار شبكة الانترنت.

موجز قصير عن التشفير الترميز

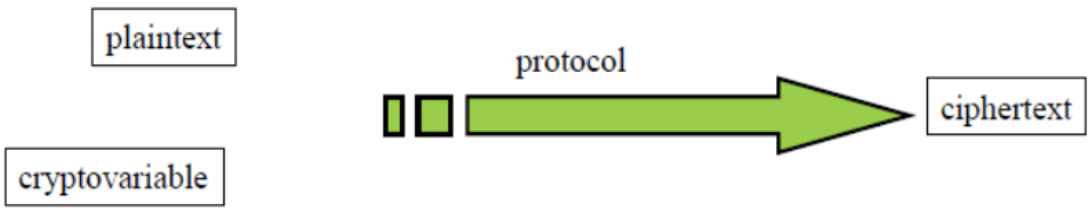
ما المقصود بالتشفير؟

- **موسوعة بريتانيكا:**
- "التشفير: ممارسة تشفير وفك رموز الرسائل في الكود السري لجعلها غير مفهومة للجميع باستثناء المستقبل المقصود".
- **"الكتابة المخفية"**
- استخدم حتى وقت قريب كأداة عسكرية
- وكأي تقنية عسكرية أخرى: فقد تغير بمرور الزمن
- **جانبي التشفير:**
- تصميم الأكواد (التشفير)
- فك الأكواد (تحليل الشفرات)
- غيرت الحواسيب كلا الجانبين

كيف نقوم بعملية الترميز؟

البروتوكول أو الخطة: طرق الترميز .

قابل للتشفير أو المفتاح: معلومات سرية



التشفير بالمفتاح المتناظر وفك التشفير هو نفس الشيء

استخدام التشفير في الحضارة السومرية

- 3500قبل الميلاد : السومريين

- الكتابة المسمارية

استخدام التشفير في الحضارة المصرية

- 1900قبل الميلاد : مصر
- أول من عرف استخدام التشفير

استخدام التشفير في الحضارة اليونانية

- 486قبل الميلاد : اليونان
- .–Σκυτάλη skee tah lee

استخدام التشفير في الحضارة الرومانية

- 50-60 قبل الميلاد : يوليوس قيصر

شفرة الاستبدال

- تحويل الحروف بمواضع:x
- مثال... A □D, B□E, C□F, : E.g. X = 3:

- ما هي نقاط الضعف؟
- تحليل التكرار (١٠٠٠ م(
- 1466ليون أربنتيني: قرص الشفرة
- استخدمت حتى القرن السادس عشر

مثال شفرة قيصر

- البروتوكول: تحويل كل حرف بنفس المقدار .
- القابل للتشفير: مقدار التحويل

Veni, vidi, vici → Foxs, fsns, fsms

- فك التشفير: فك التحويل بنفس المقدار
- الحالة الأولى: في حال عدم معرفتنا البروتوكول
- مشكلات عويصة عند تحليل الشفرات
- الحالة الثانية: في حال معرفتنا بالبروتوكول

- نحتاج لتخمين إمكانية فك الشفرات
- يوجد ٢٦ احتمال فقط
- محمد بن موسى الخوارزمي

- علم فلك ورياضيات مسلم ومنجم وعالم جغرافيا.
- طور مفهوم الخوارزميات في
- علم الرياضيات.
- يعتبر علم الجبر الذي وضع أساسه الخوارزمي أساس وحجر الأساس هذا العلم
- "ندين للخوارزمي باختراعه علم الجبر
- مقتبس من كتاب "المختصر في حساب الجبر والمقابلة"
- الكندي

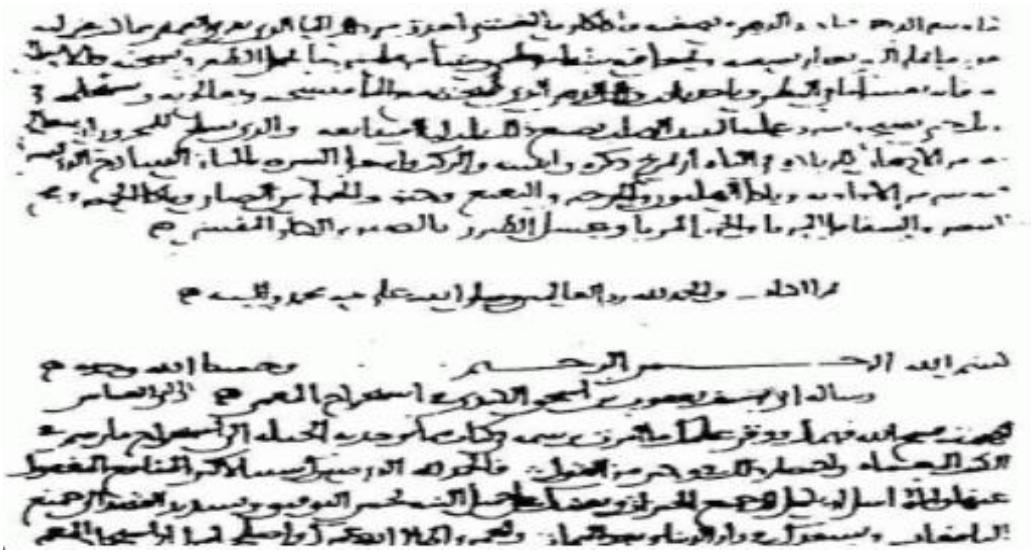
- علم التشفير الحديث الذي نشأ بين العرب، وكانوا أول من يوثقون طرق التشفير بشكل منهجي.

- الكندي: عالم رياضيات مسلم، وُلد حوالي عام ٨٠٠م اخترع تقنية تواتر الحروف لفك شفرات الاستبدال احادية الأبجدية

- أثبت أهمية التقدم ال ١ي أحرزه في هذا العلم حتى الحرب العالمية الثانية.

رسالة في استخراج المعمّى

- ألف الكندي كتاباً في علم التشفير بعنوان "مخطوطة فك رسائل التشفير" والذب وصفها بأن تكون أول التقنيات التشفيرية، وتشمل بعض الشفرات متعددة الأبجدية وتصنيف التشفير وعلم الصوتيات العربي وعلم التراكيب وأكثرهم أهمية، وضع أول اوصافه عن تواتر الحروف.



- غطى ايضاً طرق التشفير، وتحليل شفرات بعض الشفرات، والتحليل الاحصائي للحروف وبعض تركيبات الحروف في اللغة العربية.

أحمد القلقشندي

- تاريخ الميلاد: ١٣٥٥-١٤١٨
- ألف كتاب صبح الأعشى
- موسوعة تتكون من ١٤ جزء ويشتمل على قسم في التشفير.
- تم استقاء هذه المعلومة من العالم ابن الدريهم، الذي عاش في فترة من عام ١٣١٢وحتى ١٣٦١ ولكن فقدت مؤلفاته عن علم التشفير.

- شفرة فجنير
- العالم بليز دو فجنير (المولود عام ١٥٨٧ م)
- شيفرة متعددة الأبجدية: العلاقة واحد إلى متعدد
- مثال.
- الكلمة المشفرةlamp :
- كلمة السرubc :
- النص المشفرfboj :
- قام بفك الشفرة العالم بابيج وكاسيسكي (١٨٦٣م)
- اكتشاف طول كلمة السر
- تقسيم الرسالة إلى قطع استبدال مشفرة
- استخدام تواتر الحروف لحلها

مورس

- ١٨٤٥:
- شفرة مورس
- عرض إشارة مشفرة
- حالات(التشغيل والإطفاء) المكونة من ٥ رموز
- ADFGVX
- 1918:
- شفرةADFGVX
- استخدمها الجيش الألماني في الحرب العالمية الأولى

	A	D	F	G	X
A	B	T	A	L	P
D	D	H	O	Z	K
F	Q	F	V	S	N
G	G	J	C	U	X
X	M	R	E	W	Y

- **آلة إنجما**

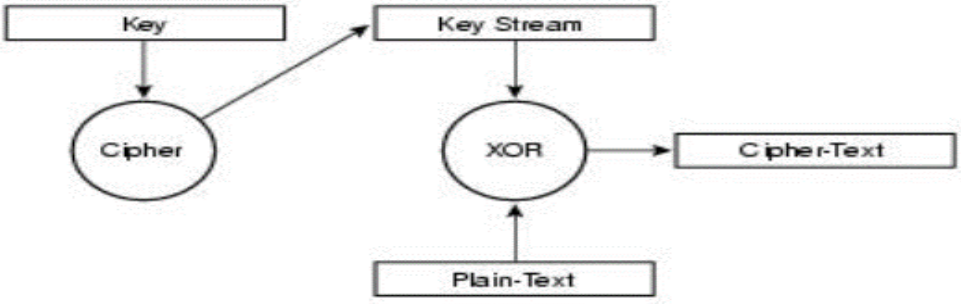
- **نظام تشفير استخدمته ألمانيا في الحرب العالمية الثانية.**
- **الفكرة: تعديل الخطابات**
- قرص تشويش يستخدم لعملية التبديل
- يقوم بالدوران بعد كل حرف، يستخدم الكثير من عمليات التبديل
- عمليات تبديل إضافية، باستخدام لوحة المفاتيح
- آلان تورنغ: لوحة مفاتيح محولة
- تمكن البريطانيون من قراءة الرموز
- قسم تكنولوجيا المعلومات والاتصالات
- المتحدثون بشفرة نافاجو
- استخدمها الأمريكان في حرب المحيط الهادئ أثناء الحرب العالمية الثانية.
- وكان لدى كل فصيلة واحداً من شعب نافاجو
- وبالرغم من كشف النظام، إلا أن اليابانيون لم يستطيعوا فك الشفرات
- مثل لوحة المرة الواحدة: يعد السر المحبك مسبقاً، لغة كاملة
- ربما بلا يمكن استخدامها في الوقت الحالي

علم التشفير الحديث

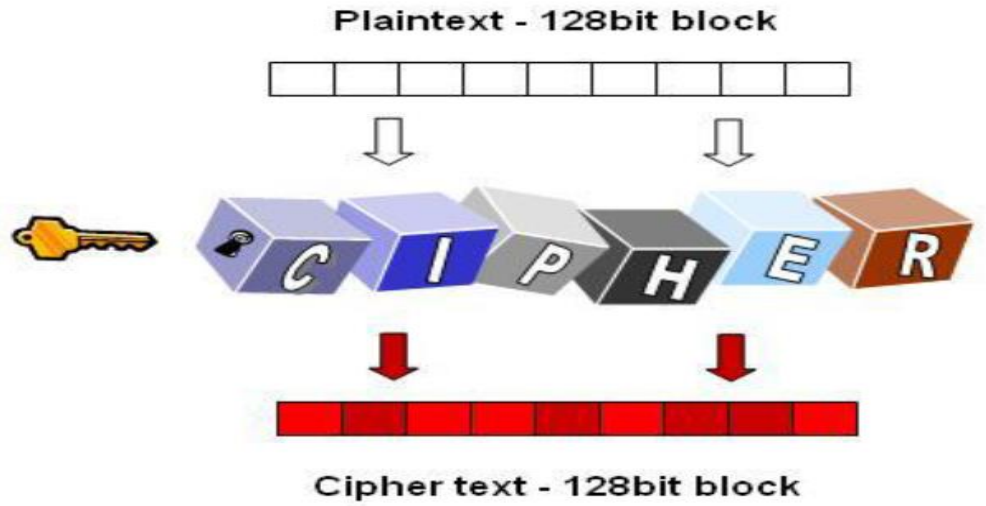
- 1949شانون
- نظرية الاتصال لنظم الأسرار
- خوارزمية رياضية تحول النص المجرد إلى نص مشفر، لأغراض أمنية
- افتراض أن الأعداء قاموا بكشف البروتوكول
- ويكون المفتاح وحده سر
- التشفير، استخدام أجهزة الحاسوب لتحليل الشفرات
- متاحة للجميع، السماح للجميع بمحاولة فك الشفرة
- دائما يفشل التصميم المغلق (الهواتف النقالة(
- المصطلحات الأساسية والمسائل الموضحة
- دراسة حالة: الفيروس المنتقل ستوكسنت

تشفير بالمفتاح المتناظر

- خوارزمية واحدة قوية
- يجب أن يظل مفتاحين سراً
- تشفير تدفقي
- سلسلة المفتاح. عمليةXOR
- التغذية المرتدة الخطية
- التغذية المرتدة غير الخطية
- مولد ستوب أند جو
- المولد المتقلص



- التشفير الكتلي
- شفرة فيستيل ثابتة الطول
- دالة الجولة
- معيار تشفير البيانات
- مقاييس التشفير المتقدمة



- تحليل الشفرات والمهتمون بالتشفير
- هجوم النص المشفر. نوعان
- المحترف والهاوي
- نقاط الضعف
- هجوم عنيف
- تحليل الشفرات الخطية
- تحليل التعمية التفاضلي

- التشفير المتناظر وغير المتناظر
- التشفير المختلط
- خصوصية جيدة جداً
- خصوصية جيدة جداً مفتوحة

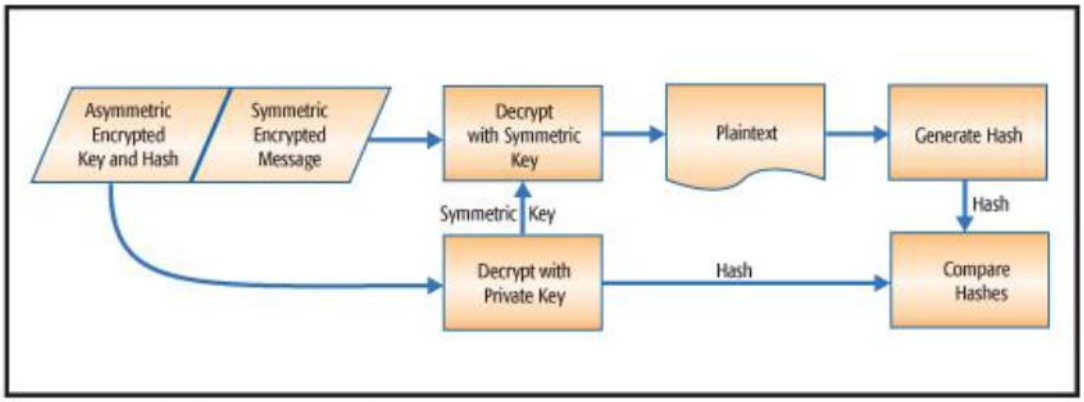
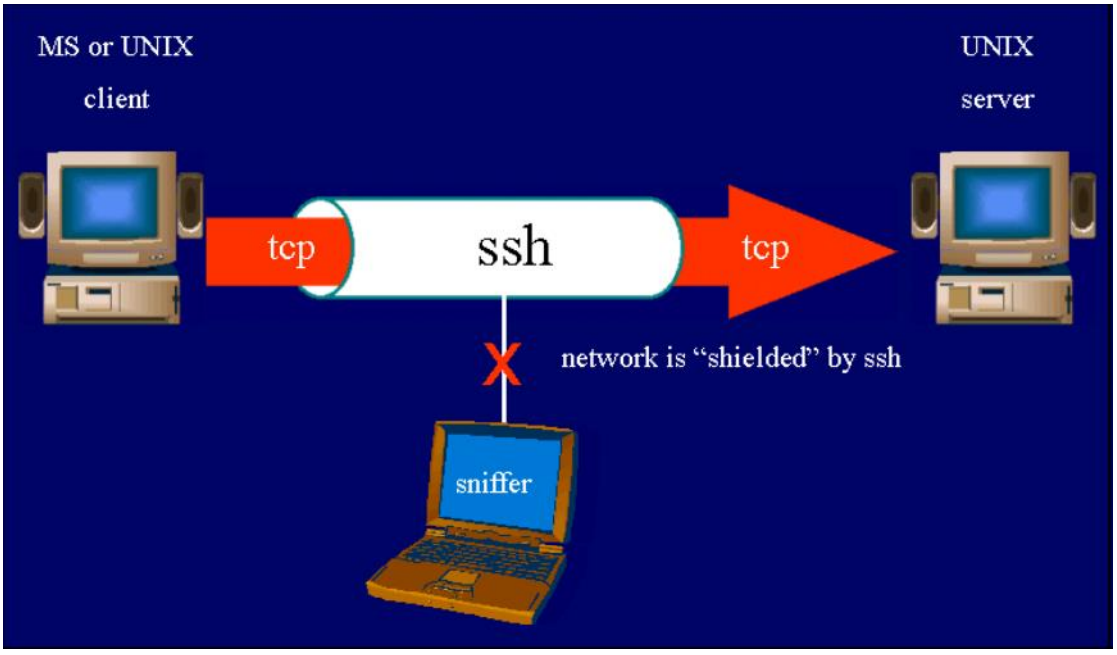


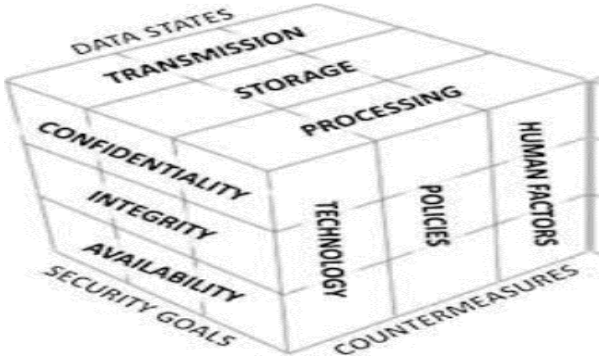
FIGURE 3 | Decryption with a hybrid cryptosystem

- سجلات الدخول المشفرة
- بروتوكول النقل الآمن
- تسجيل دخولR
- كيربيروس
- طوابع زمنية
- مفتاح جلسة العمل
- مفتاح سري

- تجزئة من ناحية واحدة



- دراسة حالة:
- فيروس متنقل ستوكسنت
- ستوكسنت
- فيروس متنقل ضار، والتي ظهرت لأول مرة عام ٢٠١٠.
- وظل في مرحلة التطور منذ عام ٢٠٠٥ على الأقل
- يستهدف أنظمة سكادا -عناصر التحكم المنطقية القابلة للبرمجة
- يُعتقد انها المسؤولة عن التلف الفعلي لبرنامج إيران النووي.
- شاهد مقطع الفيديو وناقش.
- اليوم الأول: نظرية الأمن الإلكتروني
- ورشة عمل للتوعية بشأن أمن المعلومات، خريف ٢٠١٨
- البعد الثالث للأمن الإلكتروني
- مكعب الأمن الإلكتروني



الأهداف الامنية

- يُعرف البعد الأول بمكعب الامن الإلكتروني الأهداف لحماية العالم الإلكتروني. كما تُحدد أهداف البعد الأول المبادئ الأساسية لعالم الأمن الإلكتروني.
- وهناك ثلاثة مبادئ ألا وهي السرية، والتكامل والتوفر.
- توفر هذه المبادئ التركيز لمتخصصي الأمن الإلكتروني وتتيح لهم فرض وضع أولويات لإجراءاتهم تجاه حماية العالم الإلكتروني.
- استخدم الاختصار CIA لتتذكر الثلاثة مبادئ.
- السرية

- تمنع السرية الإفصاح عن المعلومات والموارد والعمليات لغير المسؤولين. وهناك تعبير آخر يستخدم بدلاً من السرية ألا وهو الخصوصية.
- تحتاج المؤسسات إلى تدريب موظفيها على أفضل ممارسات حماية المعلومات الحساسة لحماية أنفسهم ومؤسساتهم من الهجوم.
- تستخدم هذه الأساليب لضمان السرية بما في ذلك تشفير البيانات، والمصادقة والتحكم بالوصول.
- خصوصية البيانات
- تجمع المؤسسات مجموعة كبيرة من البيانات وتكون الكثير من هذه البيانات غير حساسة لأنها متوفرة للجميع، مثل الأسماء وأرقام الهاتف.
- فعلى الرغم من أن البيانات الأخرى المُجمعة حساسة. وتعتبر المعلومات الحساسة بيانات مؤمنة من الوصول غير المصرح لحماية الفرد أو المؤسسة.
- وتبدو كلاً من السرية والخصوصية، ولكن من وجهة نظر قانونية، فإنهم يعنوا شيئين مختلفين.
- فمعظم البيانات خاصة، ولكن ليس جميعها سري.
- كما تحتوي المعلومات السرية على حالة خاص.
- وتتعلق الخصوصية باستخدام البيانات الملائمة.

التحكم بالوصول

يُعرف عدد من مخططات الحماية التي تمنع الوصول غير المرخص لجهاز الكمبيوتر، أو قاعدة البيانات، أو موارد البيانات الأخرى. وتشترك مبادئ AAA الثلاثة في خدمات التأمين:

- **المصادقة** تتحقق من هوية المستخدم لمنع الوصول غير المُرخص.
- **خدمات التخويل** تُحدد الموارد التي يستطيع المستخدمين الوصول لها بالإضافة إلى العمليات التي يستطيع المستخدمين القيام بها. ويستطيع التخويل التحكم عند وصول المستخدم إلى مورد مُحدد.
- **المحاسبة** تتعقب ما يفعله المستخدمون بما في ذلك ما يصلون له وكم من الوقت يستغرقون أثناء الاطلاع على الموارد والتغييرات التي يقومون بها.

التكامل

- مبدأ تكامل البيانات: التكامل هو الدقة، والاتساق، وموثوقية البيانات أثناء دورة الحياة الحالية.
- وهناك تعبير آخر يستخدم بدلاً من التكامل ألا وهو الجودة.
- تستخدم الأساليب لضمان تكامل البيانات بما في ذلك التجزئة، والتحقق من صحة البيانات، والتحقق من اتساق البيانات، وأدوات التحكم بالوصول.
    - الحاجة إلى تكامل البيانات.
- يعتبر حماية تكامل البيانات تحدي ثابت بمعظم المؤسسات.
    - التحقق من التكامل

هو أسلوب لقياس اتساق مجموعة البيانات.

التوفر

- يعتبر توفر البيانات مبدأ مستخدم لوصف الحاجة للحفاظ على توفر أنظمة المعلومات والخدمات بجميع الأوقات.
- تستطيع الهجمات عبر الإنترنت وفشل الانظمة منع الوصول لأنظمة المعلومات والخدمات.
- تستخدم الأساليب لضمان التوفر بما في ذلك تكرار النظام، ونسخ النظام الاحتياطية، ومرونة النظام المتزايدة، وصيانة المعدات، وأنظمة التشغيل والبرامج الحديثة، والخطط المناسبة لاسترداد ما ضاع من معلومات المفاجئ بسرعة.
- وتحتوي الانظمة عالية التوفر على ثلاثة مبادئ للتصميم: استثناء نقاط الخطأ الفردية، وتوفير النقل الآمن، والكشف عن الأخطاء التي قد تحدث.

عدم الإنكار

- لن تستطع المؤسسة نفي (إنكار) الإجراءات السابقة
- حيث يعتبر عدم الإنكار هو القدرة على إثبات أو عدم إثبات أن شيء حدث مثل المعاملات المالية أو ضم التوقيعات باتفاقية قانونية.
- ولهذا الأمر جذور بالعمليات القانونية وذلك لمنع الكيانات من الادعاء بعدم الموافقة على شيء أو توقيع مستند.

حالات البيانات

- العالم الإلكتروني هو عالم البيانات.
- يُركز متخصصو التأمين الإلكتروني على حماية البيانات.
- ويُركز البعد الثاني من مكعب التأمين الإلكتروني على مشكلات حماية جميع حالات البيانات ضمن العالم الإلكتروني.
- وتتضمن البيانات ثلاثة حالات محتملة:
  ١) البيانات المحتجزة أو المُخزنة
  ٢) البيانات المنقولة
  ٣) البيانات قيد المعالجة

بيانات ثابتة

- تعني البيانات الثابتة أن نوع من جهاز التخزين يحتفظ بالبيانات عندما تستخدمها العملية.
- البيانات التي تم تخذينها تشير إلى البيانات الثابتة.
- يمكن لجهاز التخزين ان يكون محلي (على جهاز حاسوبي) أو مركزي (على الشبكة.(
- أجهزة التخزين المرتبط بالشبكات
- مصفوفة التعدد للأقراص المستقلة
- التخزين الشبكي
- شبكة منطقة النظام

بيانات متنقلة

- يتضمن نقل البيانات إرسال المعلومات من جهاز إلى الأخر.
- هناك العديد من الوسائل لنقل المعلومات بين الأجهزة والتي تضمن علي:
- نقل البيانات عن طريق الساعي -تستخدم الوسائط القابلة للإزالة لتحريك البيانات من حاسبو إلى الأخر
- الشبكات التلقائية -تستخدم الكابلات لنقل المعلومات
- الشبكات اللاسلكية-تستخدم الموجات الكهرومغناطيسية لنقل البيانات.
- حماية البيانات المنقولة أحد أكثر الوظائف أمن الانترنت صعوبة.

وأكبر الصعوبات هي:

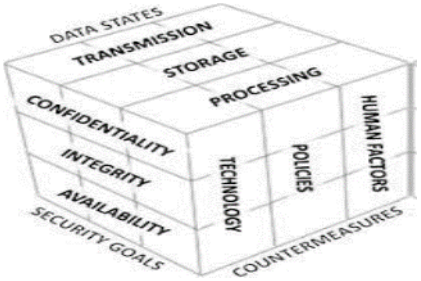
- حماية سرية البيانات
- حماية نزاهة البيانات
- حماية توفر البيانات

بيانات قيد المعالجة

- الحالة الثالثة من البيانات هي البيانات قيد المعالجة.
- هذا يشير إلى البيانات خلال المدخلات الأولية أو التعديل أو الحوسبة او المدخلات.
- تبدأ حماية نزاهة البيانات من المدخلات الأولية للبيانات.
- وسائل تجميع البيانات مثل إدخال البيانات يدوياً ونماذج المسح الضوئي ورفع البيانات والبيانات المجمعة من أدوات الاستشعار، يشكل تهديدات محتملة إلى نزاهة البيانات.
- يشير تعديل البيانات إلى أي تغير في البيانات الأصلية مثل تعديل المستخدمين للبيانات يدوياً ومعالجة البيانات وتغير البيانات وفشل المعدات المتسببة في تعديل البيانات
- ترميز/ فك الترميز
- ضغط/فك الضغط
- التشفير / فك التشفير

الإجراءات المضادة (عوامل الحماية)

- يُعرف البعد الثالث بمكعب الامن الإلكتروني يحدد أنواع السلطات المستخدمة لحماية العالم الإلكتروني.
- يحدد مكعب السحر الانواع الثلاثة من السلطات:



- التكنولوجيات -الأجهزة والمنتجات متاحة لحماية أنظمة المعلومات وتحاشي مجرمي الأنترنت.

- السياسات والممارسات -الإجراءات والإرشادات التي تمكن مواطنين عالم الانترنت من البقاء في حالة من الأمن واتباع الممارسات الحسنة
- الأشخاص -الذين على دراية ووعي بعالمهم والمخاطر التي تهدد عالمهم.

التكنولوجيات

- **تكنولوجيات الحماية المستندة إلى البرامج**
  - مكافحة الفيروسات وجدار الحماية ومكافحة البرامج الضارة وتصفية المحتوى

- **تكنولوجيات الحماية المستندة إلى الأجهزة**
  - أنظمة الكشف عن محاولات التدخل وأنظمة منع محاولات التدخل وتصفية المحتوى

- **تكنولوجيات الحماية المستندة إلى الشبكة**
  - الشبكة الخاصة الظاهرية
  - التحكم في الدخول إلى شبكة
  - أمن نقطة الوصول اللاسلكي

- **تكنولوجيات الحماية المستندة إلى السحابة**
  - البرامج كخدمة
  - البنية الأساسية كخدمة
  - أجهزة الأمان الظاهرية

التعليم والتدريب في مجال أمن الأنترنت

- يعد برنامج التوعية بالأمن في غاية الاهمية للمؤسسات.
- قد لا يقصد الموظف الضرر ولكنه يجهل الإجراءات الواجب تنفيذها .
- هناك العديد من الطرق لتنفيذ برنامج تدريبي رسمي:
- إقامة برنامج لرفع الوعي في مجال الامن كجزء من عملية الإلحاق الفعلي بالعمل.
- ربط الوعي بمجال الامن بمتطلبات الوظيفة أو تقييم الأداء

- عقد دورات تدريبية بصفة شخصية
- إكمال دورات عبر الانترنت
- تكون عملية التوعية في مجال الأمن عملية مستمرة!

السياسات والإجراءات الخاصة بمجال أمن الأنترنت

- سياسات الأمن هي مجموعة من الأغراض الأمنية للشركة التي تضمن قواعد السلوك للمستخدمين والمديرين وتحدد متطلبات النظام.
- هذه الأغراض والقواعد والمتطلبات تكفل بصورة جماعية أمن الشبكات والبيانات وأنظمة الحاسوب في المؤسسة.
- تساعد المعايير موظفي تكنولوجيا المعلومات للحفاظ على الاتساق في تشغيل الشبكات .
- الإرشادات هي قائمة من الاقتراحات حول كيفية القيام بالأشياء بصورة أكثر فاعلية وبأمان.
- وتكون وثائق الإجراءات أطول وأكثر تفصيلا من المعاير والإرشادات.

التحكم في الوصول

ورشة عمل للتوعية بشأن أمن المعلومات خريف ٢٠١٨

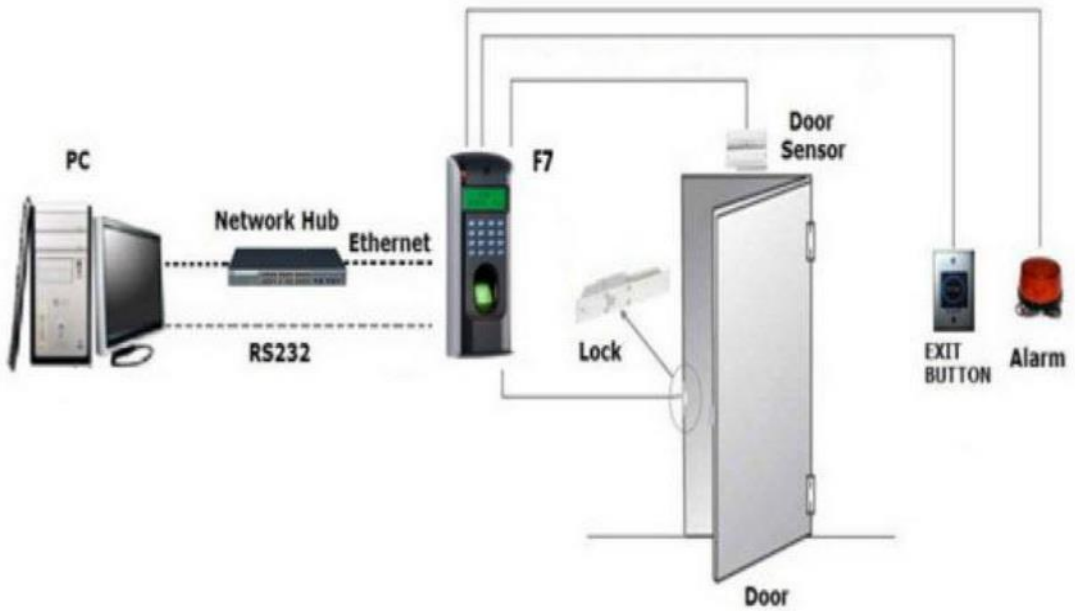
ما هو التحكم في الوصول

أمثلة:


أمثلة على البرامج:

المفاهيم

المستخدمين والمجموعات التصديق

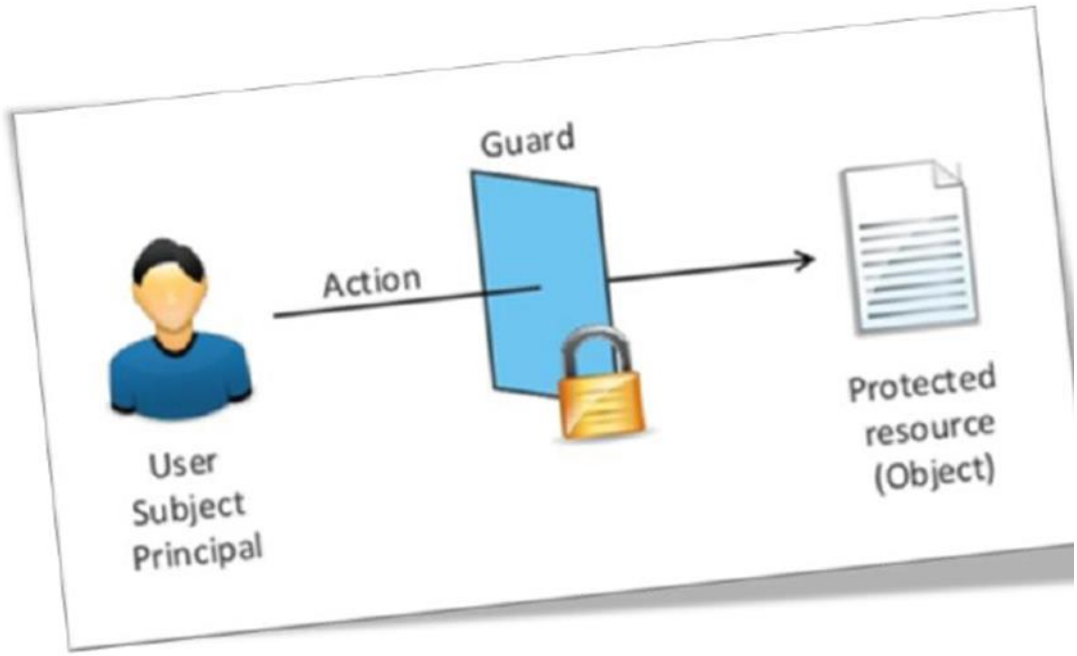


- كلمات المرور
- حماية الملف
- قوائم التحكم في الوصول

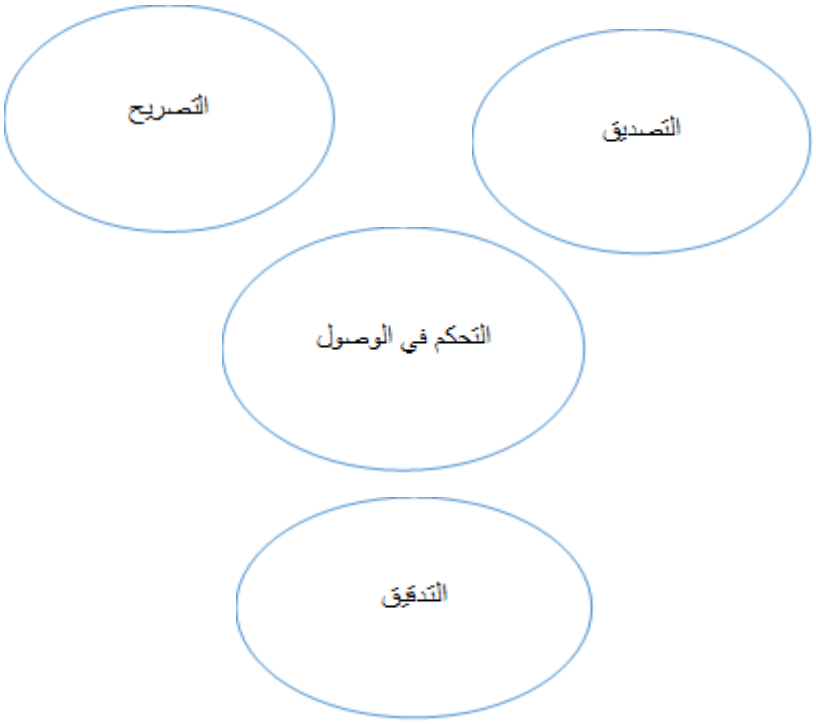
الأسئلة

- أي من المستخدمين يستطيع قراءة /كتابة أي من الملفات؟
- هل ملفاتي بأمان فعلاً؟
- وماذا يعني أن تكون جذري؟
- ما الذي نريد التحكم به؟

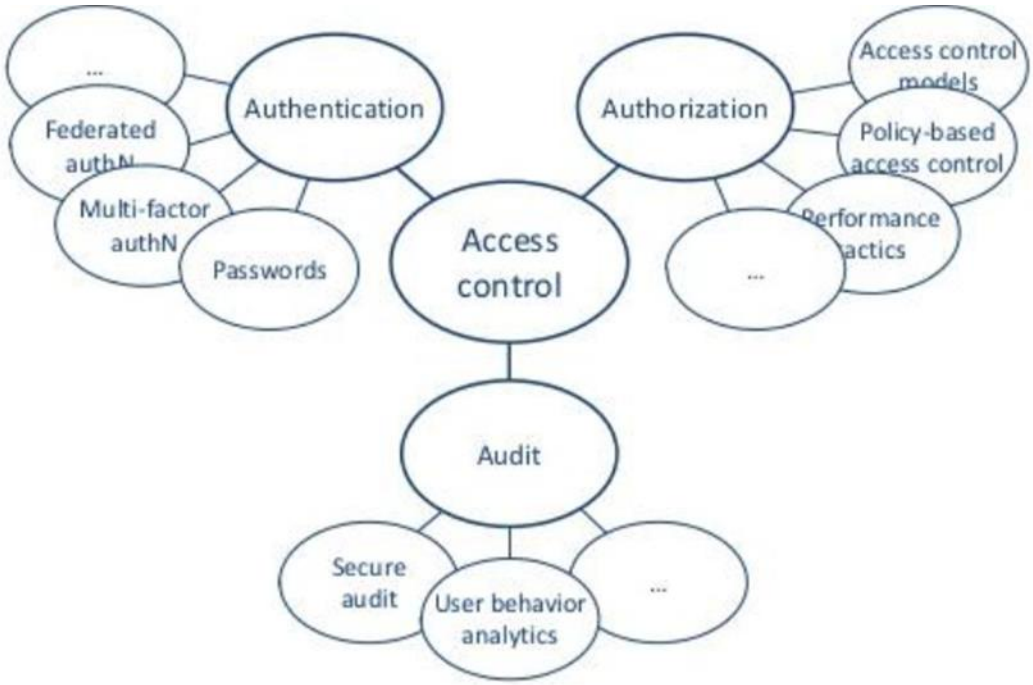
نظرة عن بعد:



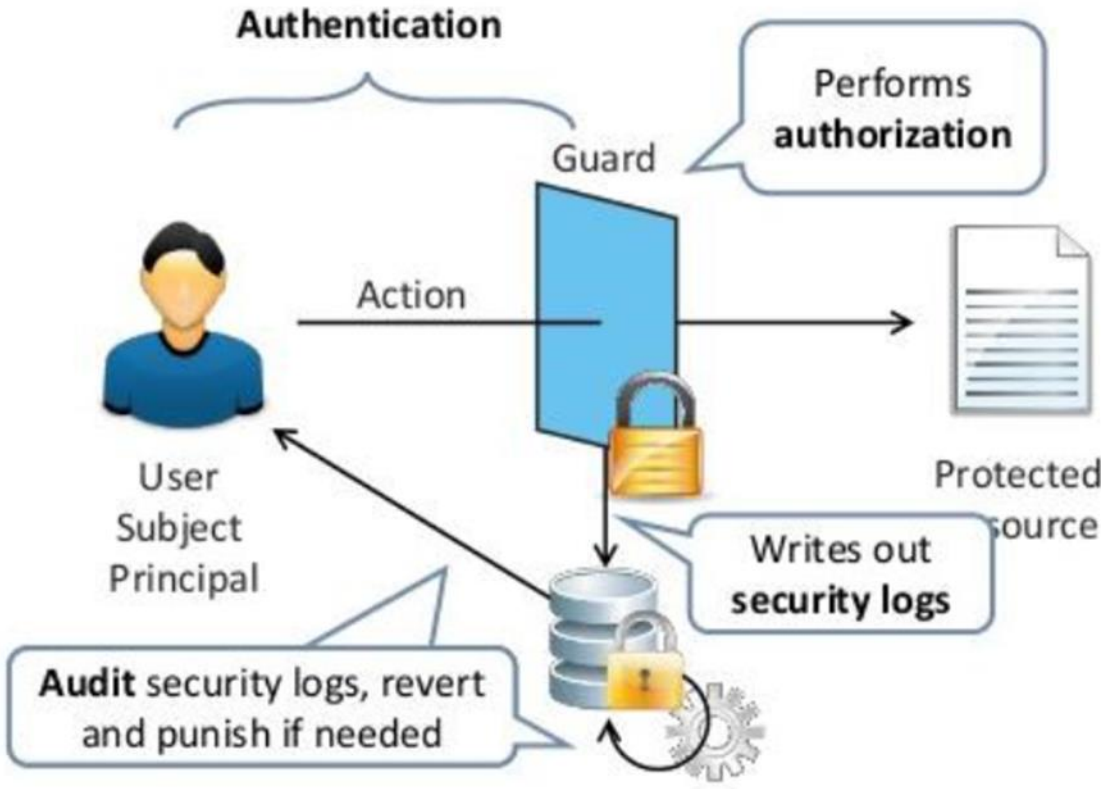
بعض التفاصيل:



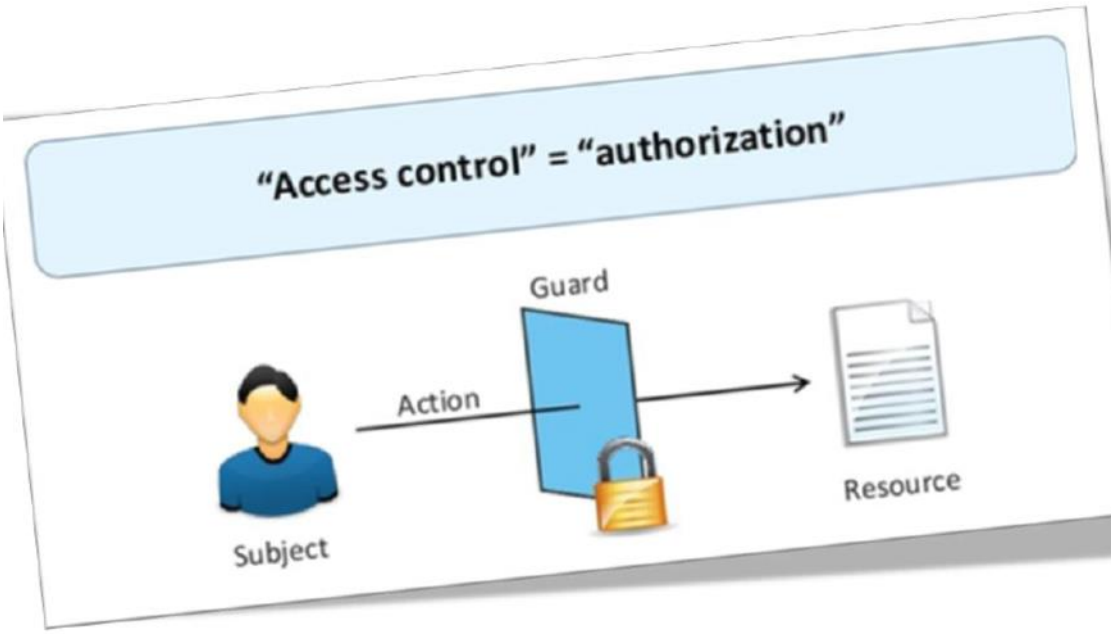
المزيد من التفاصيل



نظرة عن كثب:



أخيراً:



التصديق

- يتحكم التصديق فيما يمكن للمستخدم فعلة وما يعجز عن فعلة على الشبكة بعد القيام بعملية التصديق بنجاح:

بعد ما يقوم المستخدم بأثبات هويته، يتفقد النظام موارد الشبكة التي يمكن للمستخدم الوصول إليها وما يستطيع المستخدم فعلة بهذه الموارد.

- يستخدم التصديق مجموعة من السمات التي تصف وصول المستخدم إلى الشبكة.
- يقوم النظام بمقارنة هذه السمات بالمعلومات الذي يتضمنه قاعدة بيانات المصادقة ويحدد مجموعة من القيود لهذا المستخدم وتقوم بتوصيلها إلى الموجه المحلى المتصل به المستخدم.
- وضع قواعد المصادقة هي الخطو الأولي في التحكم في الوصول. وتضع سياسة المصادقة هذه القواعد.

المحاسبة

- تتعقب المحاسبة عملية رجوعاً إلى شخص أو العملية التي تقوم بتغير في النظام وتجمع المعلومات وتقدم تقارير بشأن استخدام البيانات:
  - تستخدم المؤسسة هذه البيانات لهذه الأغراض مثل التدقيق أو تقديم الفواتير.
  - تتضمن البيانات المجمعة وقت تسجيل المستخدم سواء كانت عملية التسجيل ناجحة او باءت بالفشل، كما تتضمن موارد الشبكة التي توصل إلها المستخدم.
  - يسمح هذا للمؤسسة بتعقب العمليات والأخطاء خلال التدقيق أو التحقيق.
  - يتكون تنفيذ المحاسبة من التكنولوجيات والسياسات والإجراءات والتعليم.
  - توفر ملفات السجل معلومات المفصلة بناء على البارامترات المختارة.

مصفوفة التحكم في الوصول

- جدول يحدد أذونات.
  - كل صف في هذا الجدول مرتبط بفاعل هو المستخدم أو المجموعة او النظام
  - الذي يمكن أن يقوم بعمليات.
  - كل عمود في هذا الجدول مرتبط بكائن وهو الملف أو الدليل أو ال مستند أو الجهاز أو الموارد أو أي جهة أخري التي بشأنها نريد تحديد حقوق الوصول.
  - كل خلية في هذا الجدول ممتلئة بحقوق الوصول بشأن المجموعة ذات الصلة من الفاعل والكائنات.
  - أي خلية فارغة تعني عدم الحصول على حقوق الوصول.
- تتضمن حقوق الوصول العمليات مثل القراءة والكتابة والنسخ والتنفيذ والحذف والتعليق.

مثال على مصفوفة التحكم في الوصول:

	/etc/passwd	/usr/bin/	/u/roberto/	/admin/
root	read, write	read, write, exec	read, write, exec	read, write, exec
mike	read	read, exec		
roberto	read	read, exec	read, write, exec	
backup	read	read, exec	read, exec	read, exec
...	...	...	...	...

مشاكل مصفوفة التحكم في الوصول

قد يكون الجدول كبيراً للغاية!

مثال:

نظام Unix الذي يضم ١٠٠٠ مستخدم و١٠٠٠ مجموعة كل عملية ruid أو rgid أو egid أو ١٠٠٠٤ = تريليون من المجالات.

يمتلك نفس النظام ١٠٠٠ ملف/مجلدات أو مليون مفعول كائنات (بالإضافة إلى المستخدمين والمجموعات الأخرى).

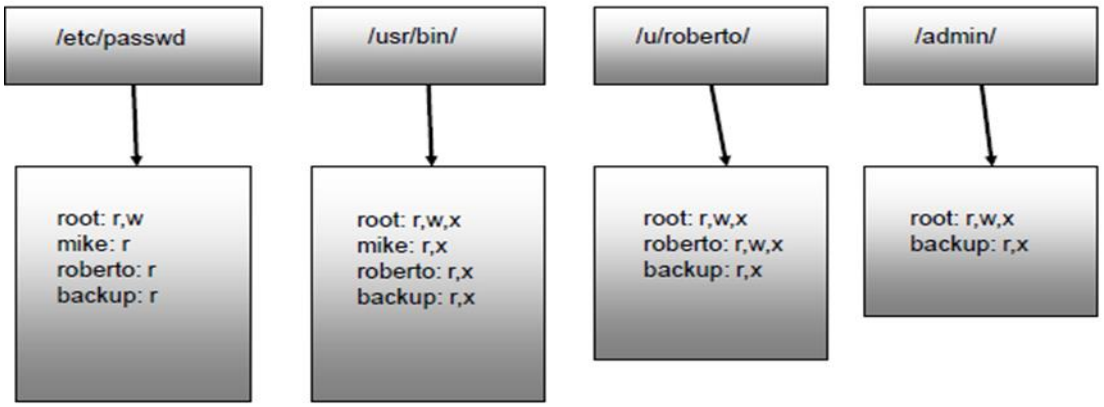
رابطة مكائن الحوسبة لديها مليون وتريليون خلية!

الحل: قوائم التحكم في الوصول

تقع مسؤولية وضع معايير الشبكات على العديد من المنظمات العالمية المختصة بوضع المعايير. من الأمثلة على هذه المنظمات : منظمة IEEE , IETF , ISO

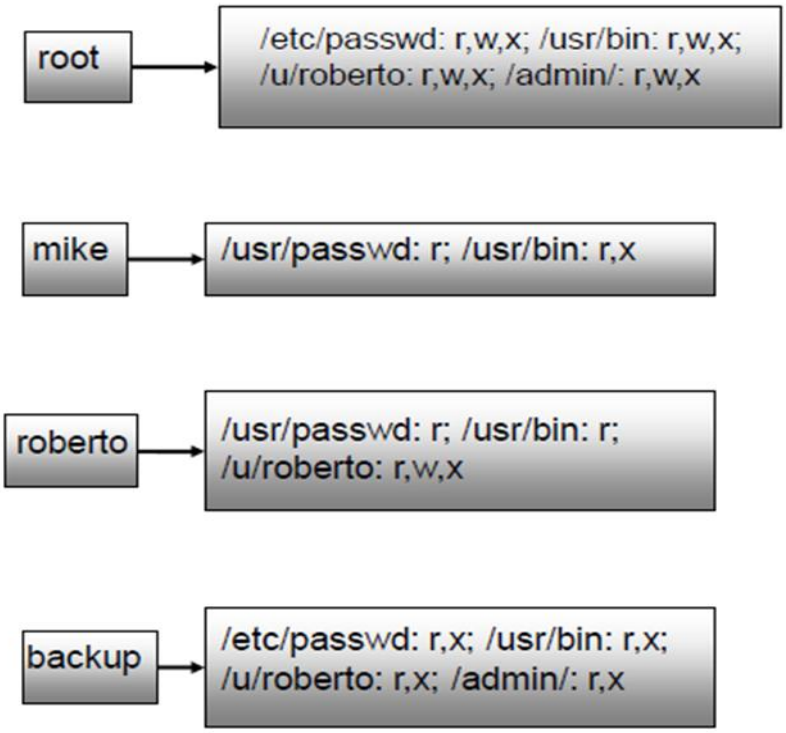
قائمة التحكم في الوصول

- تحدد لكل كائن، O، قائمة، L، تدعى قائمة التحكم الخاصة ب O والتي تسرد جميع المستخدمين الذين لديهم حقوق الوصول بشأن O ولكل مستخدم، S، يعطي حقوق الوصول التي تمنحها للمستخدم.



الامكانيات:

- أخذ منهج المستخدم المستقل للتحكم في الوصول
- يحدد لكل مستخدم S قائمة الكائنات التي لا تحمل التحكم في حقوق الدخول الفارغة بجانب الحقوق المحددة لكل كائن.



التحكم في الوصول مستند على الدور

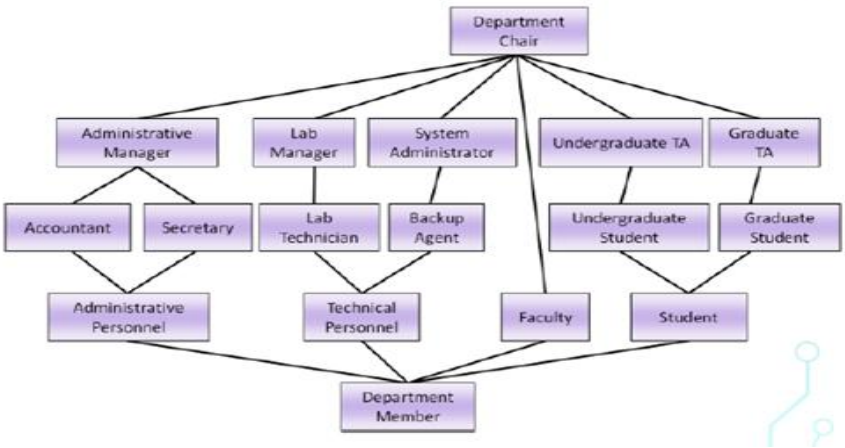
تحديد الأدوار ثم بعد ذلك تحديد حقوق التحكم في الوصول

بشأن هذه الأدوار فضلاً عن تكون مباشرة للأشخاص.

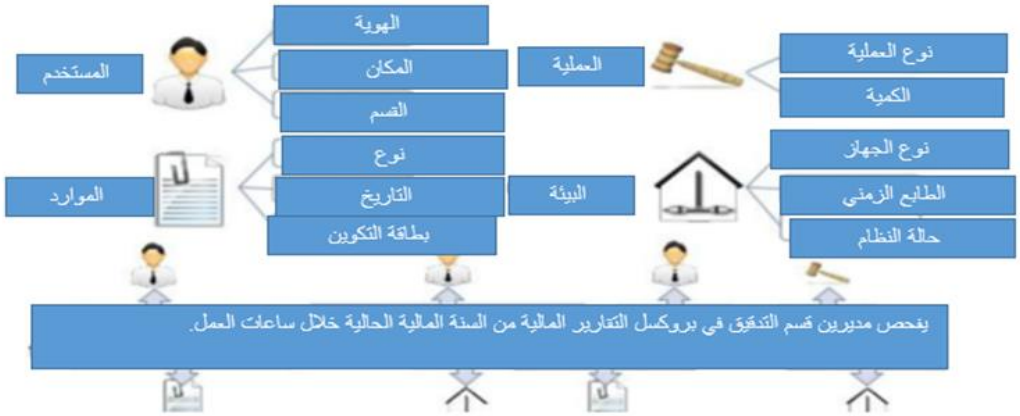
تحديد أي من هذه الأدوار يستطيع المستخدم ربط العملية.

مستوي المراوغة -إدارة الدخول عن طريق الأدوار-التعامل

مع جميع المستخدمين بهذه الدور والتعبير عن سبب الدخول (أو عدم الدخول)



التحكم في الوصول بناء على السمات:



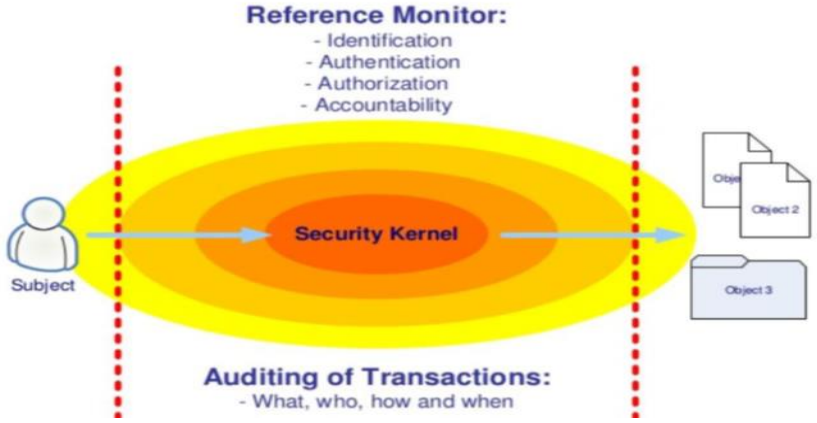
منح الأذن بذلك في حالة

المدير في أدوار المستخدمين وقسم المستخدم ==="التدقيق" ومكان المستخدم =="بروكسل" والعملية =="الفحص" ونوع الموارد =="التقرير المال" وعام الموارد" ==السنة البيئية الحالية و8ساعات 00 أصغر من الوقت البيئي أصغر من 17 ساعة 00

- تم اتخاذ قرارات الوصول بناءً على السمات
- يقصد بالسمات الصفات الأساسية ذات القيمة لمستخدم ما، والموارد والفعل أو البيئة
- تحويل النتائج إلى تحكم في الوصول المعروف النص والحركي
- يمكن أن تعبر السمات عن مختلف مفاهيم التحكم في الوصول
- الأذونات، والأدوار، والمجموعات، والاقسام، والوقت، والمكان، والملكية، والملكية ذات المجال المحدد

المصادقة التفويض المسؤولية:

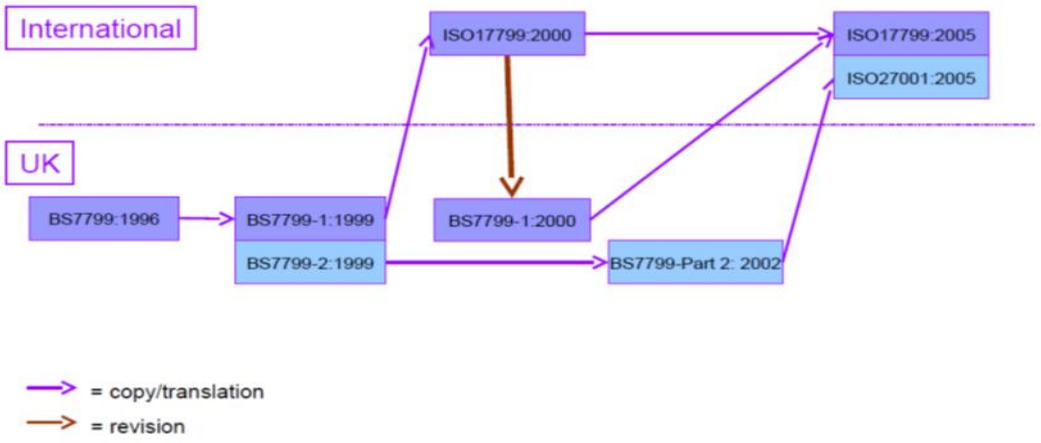
- Access control is not complete without coupled with auditing for accountability.
- Reference monitor provides the mechanism for access control. (i.e., AAA)



- ISO/IEC2700d

ورشة عمل للتوعية بشأن أمن المعلومات

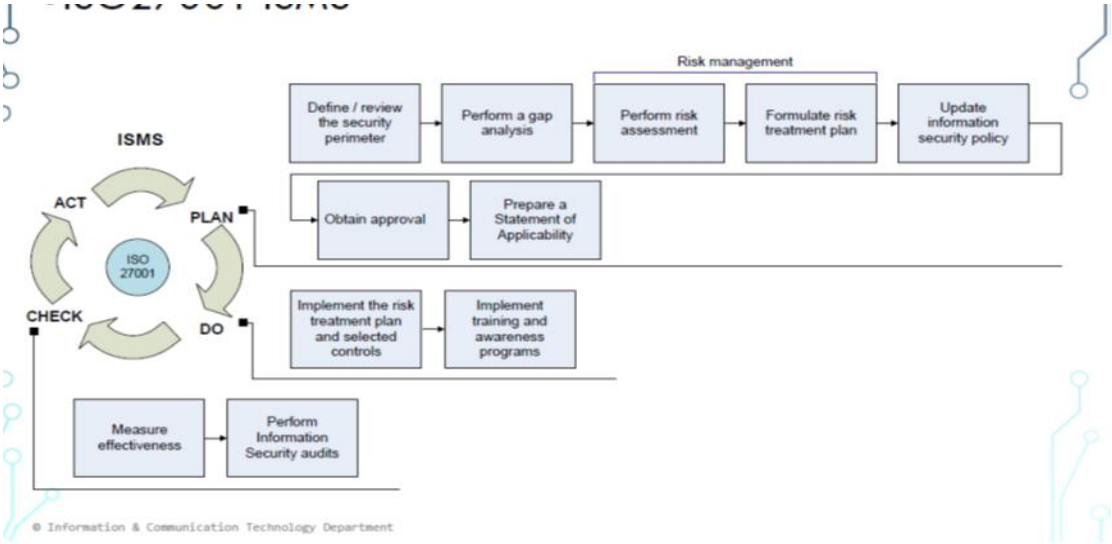
- فئة ٢٧٠٠٠
- معيار إدارة أمن المعلومات آيزو/ آي إي سي الوصف
- 27000 المرادف والتعريف
- 27001 مواصفات (BS7799-2) الصادرة في أكتوبر ٢٠٠٥
- 27002 قانون ممارسة(ISO17799:2005)
- 27003 إرشادات تنفيذية
- 27004 المقاييس والقياسات
- ٢٧٠٠٥ إدارة المخاطر (BS 7799-3)
- تاريخ آيزو ٢٧٠٠١



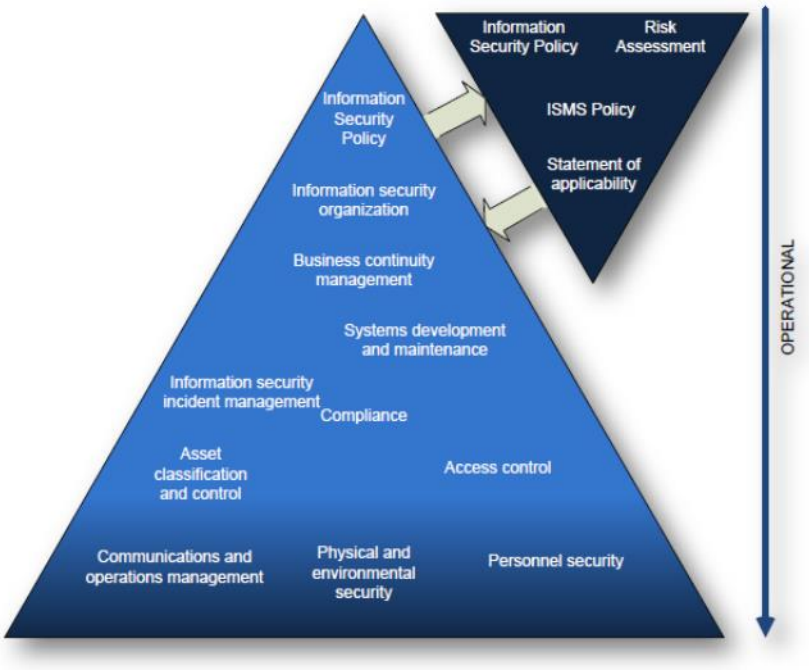
آيزو ٢٧٠٠٠ معايير الحماية

آيزو 27001	يحدد آيزو 27001 نظام الإدارة الذي يهدف إلى جلب أمن المعلومات تحت الرقابة الإدارية الصريحة.
آيزو 27002	تقدم آيزو 27002 أفضل توصيات الممارسات لإدارة أمن المعلومات أو استخدامها من قِبل المسؤولون عن المبادرة بنظام إدارة أمن المعلومات أوتطبيقه أو صيانته.

آيزو ٢٧٠٠١ نظام إدارة أمن المعلومات



آيزو٢٧٠٠٢ المجالات:



الاقسام والاهداف

٢,١ البرنامج الضار والتعليمة البرمجية الضارة

التميز بين أنواع البرنامج الضار والتعليمة البرمجية الضارة.

٢,٢ الاحتيال

وصف الخطط والتقنيات والإجراءات التي يستخدمها مجرمي الانترنت.

٢,٣ الهجمات

قارن بين الوسائل المختلفة المستخدمة في الهندسة الاجتماعية قارن بين أنواع الهجوم على الانترنت المختلفة.

٢,١ البرنامج الضار والتعليمة البرمجية الضارة:

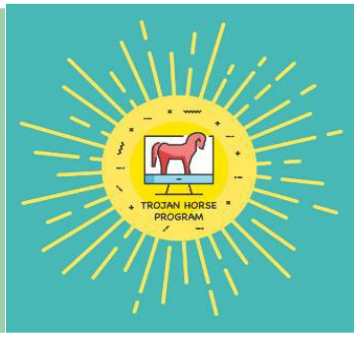
البرنامج الضاره هو مصطلح عام يتألف من مقطعين "ضار" ويعني نية الإضرار و"برنامج "

وتعني كلمة البرنامج الضار

"برنامج تم تصميمه لإلحاق الضرر بنظام الحاسوب أو الحصول على دخول مصرح"

أنواع البرامج الضاره :

أحصنة طروادة **الفيروسات الدودية** **الفيروسات**



الفيروسات:

الفيروس هو تعليمة برمجية ضارة قابلة للتنفيذ مرفقة مع ملف تنفيذي أخر.

مثل البرنامج القانوني. تحتاج معظم الفيروسات أن تطلق من قبل المستخدم النهائي وتنشط في وقت وتاريخ محددين.

الفيروسات الدودية:

الفيروسات المتنقلة هي التعليمة البرمجية الضارة التي تستنسخ عن طريق الاستغلال المستقل لمواطن الضعف في الشبكات. الفيروسات المتنقلة عادتاً ما تقلل من سرعة الشبكات. وفي حين تحتاج الفيروسات إلى برنامج مضيف لتبدأ في العمل، الفيروسات المنتقلة تستطيع العمل بمفردها. وغير الإصابة الأولية لا تحتاج الفيروسات المنتقلة إلى مشاركة المستخدم.

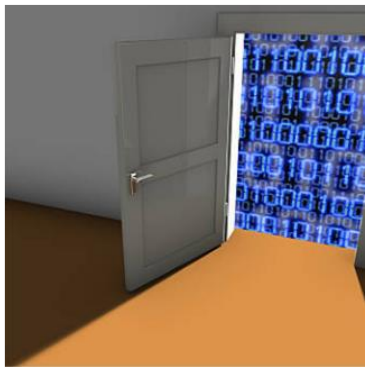
أحصنة طروادة:

حصان طروادة هو برنامج ضار يحمل عمليات ضارة على شكل عمليات منشودة مثل اللعب عبر الانترنت. تستغل التعليمة البرمجية امتيازات المستخدم التي تقوم بتشغيلها. يختلف حصان طروادة عن الفيروس لأنه الطروادة يربط نفسه بالملفات الغير قابلة للتنفيذ.

مثل ملفات الصور والملفات الصوتية او الالعاب.

انواع البرامج الضارة:

القنبلة المنطقية برنامج الفدية الضارة الأبواب الخلفية برامج الأحتيال



القنابل المنطقية:

القنبلة المنطقية هي برنامج ضار يستخدم مشغل ليقوم بتشغيل التعليمة البرمجية الضارة. على سبيل المثال قد تكون المشغلات تواريخ أو أوقات أو برامج اخري تعمل أو حذف حساب المستخدم. تظل القنبلة المنطقية غير نشطة إلى حين حدوث حدث البدء. تقوم القنبلة المنطقية بتنفيذ تعليمة برمجية ضارة التي تتسبب في إلحاق الضرر بالحاسوب.

برنامج الفدية الضارة:

يحتجز برنامج الفدية الضارة نظام الحاسوب أو البيانات التي يحتوي عليها إلى حين يقوم المستهدف بالدفع. يعمل برنامج الفدية الضارة عادتاً عن طريق تشفير البيانات في الحاسوب باستخدام مفتاح غير معرف للمستخدم.

برنامج الفدية الضارة:

الأبواب الخلفية وبرامج الاحتيال:

تشير الابواب الخلفية وبرامج الاحتيال إلى البرنامج او التعليمة البرمجية التي ادخلها المجرم الذي أخترق النظام. تتجاوز الأبواب الخلفية المصادقة الاعتيادية المستخدمة لدخول النظام.

تقوم برامج الاحتيال بتعديل نظام التشغيل لخلق باب خلفي. بعد ذلك يستخدم المهاجمون الباب الخلفي لدخول الحاسوب عن بعد.

هجمات البريد الإلكتروني والمتصفح:

البريد الإلكتروني هو خدمة عالمية يستخدمها المليارات من الأشخاص عبر العالم. واحدة من أكثر الخدمات شعبية أصبح البريد الإلكتروني يمثل موطن الضعف الأساسي للمستخدمين والمنظمات.

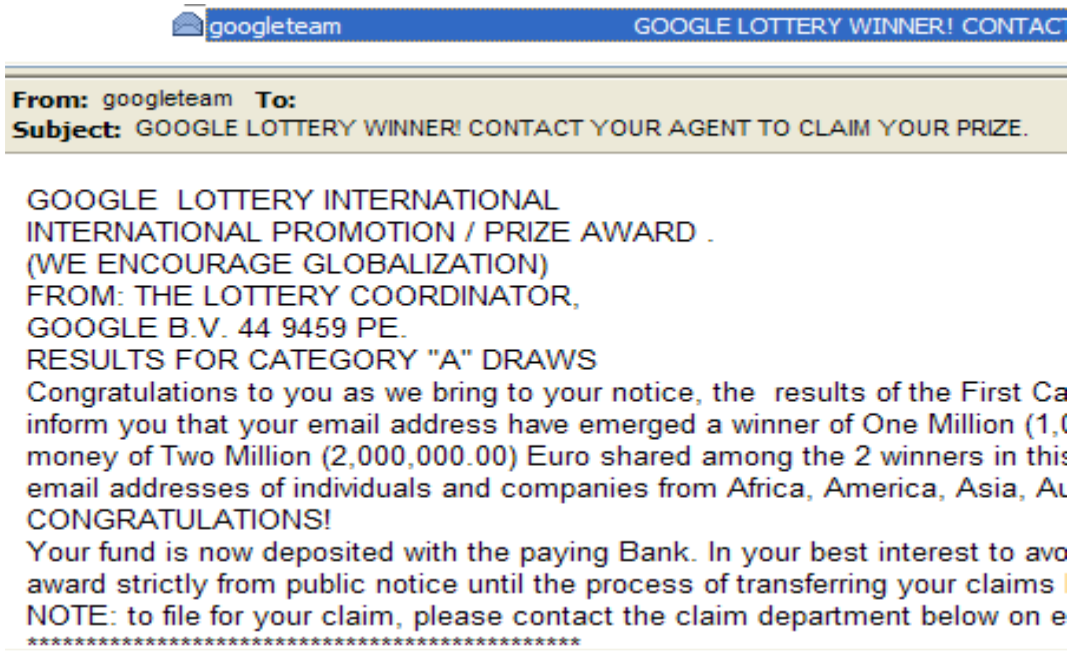
برامج التجسس:

برامج التجسس هي برامج تمكن المجرم من الحصول على معلومات حول أنشطة الكمبيوتر الخاصة بالمستخدم. غالبًا ما تتضمن برامج التجسس برامج تعقب النشاطات ، وضغط المفاتيح وجمع البيانات. في محاولة للتغلب على الإجراءات الأمنية ، تقوم برامج التجسس بتعديل إعدادات الأمان.

البريد العشوائي:

البريد المزعج ، المعروف أيضًا باسم البريد غير المرغوب فيه ، هو بريد إلكتروني غير مرغوب فيه. في معظم الحالات، تعتبر الرسائل غير المرغوب فيها طريقة للإعلان. ومع ذلك، يمكن للرسائل غير المرغوب فيها إرسال روابط ضارة أو برامج ضارة أو محتوى خادع.

مثال عن البريد العشوائي.


googleteam GOOGLE LOTTERY WINNER! CONTAC

From: googleteam **To:**
Subject: GOOGLE LOTTERY WINNER! CONTACT YOUR AGENT TO CLAIM YOUR PRIZE.

GOOGLE LOTTERY INTERNATIONAL
INTERNATIONAL PROMOTION / PRIZE AWARD .
(WE ENCOURAGE GLOBALIZATION)
FROM: THE LOTTERY COORDINATOR,
GOOGLE B.V. 44 9459 PE.
RESULTS FOR CATEGORY "A" DRAWS
Congratulations to you as we bring to your notice, the results of the First Ca
inform you that your email address have emerged a winner of One Million (1,(
money of Two Million (2,000,000.00) Euro shared among the 2 winners in this
email addresses of individuals and companies from Africa, America, Asia, Au
CONGRATULATIONS!
Your fund is now deposited with the paying Bank. In your best interest to avo
award strictly from public notice until the process of transferring your claims
NOTE: to file for your claim, please contact the claim department below on e
****

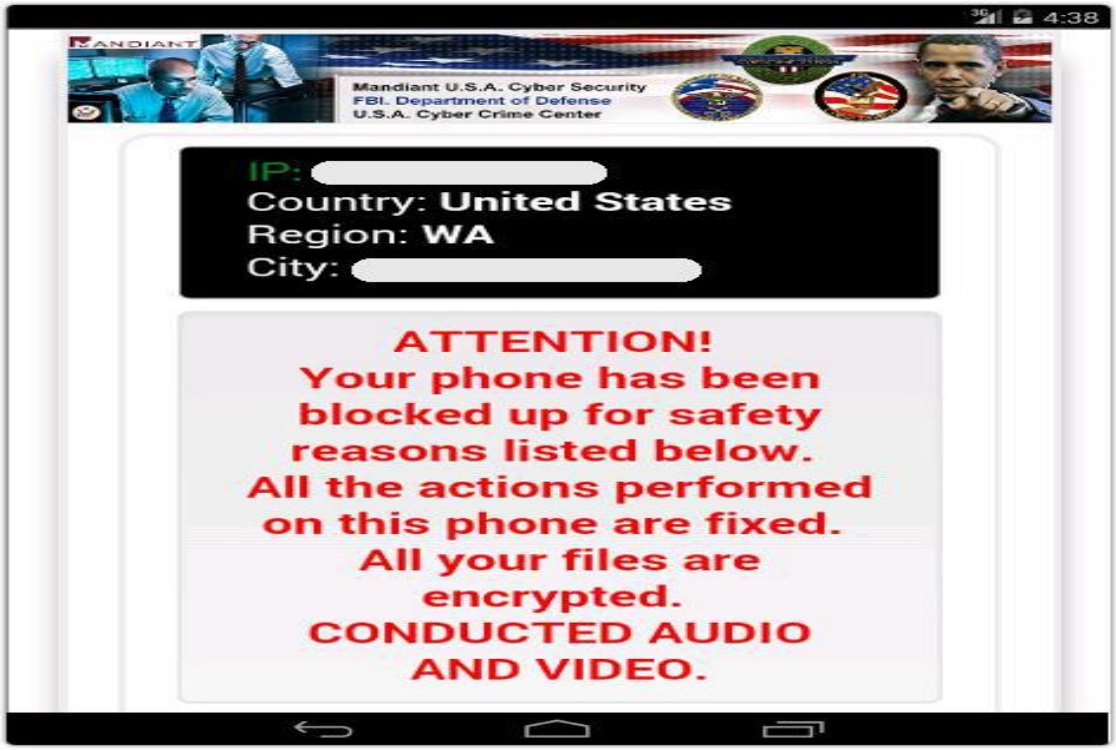
هجمات البريد الإلكتروني والمتصفح.

برامج إعلانات متسللة:

تعرض برامج الإعلانات المتسللة العناصر المنبثقة المزعجة لخلق طرق لأصحابها. قد يحلل البرنامج الضار اهتمامات المستخدم عن طريق تعقب المواقع الإلكترونية التي قام بزيارتها. وبعد ذلك يستطيع إرسال إعلانات منبثقة ذات صلة بتلك المواقع.

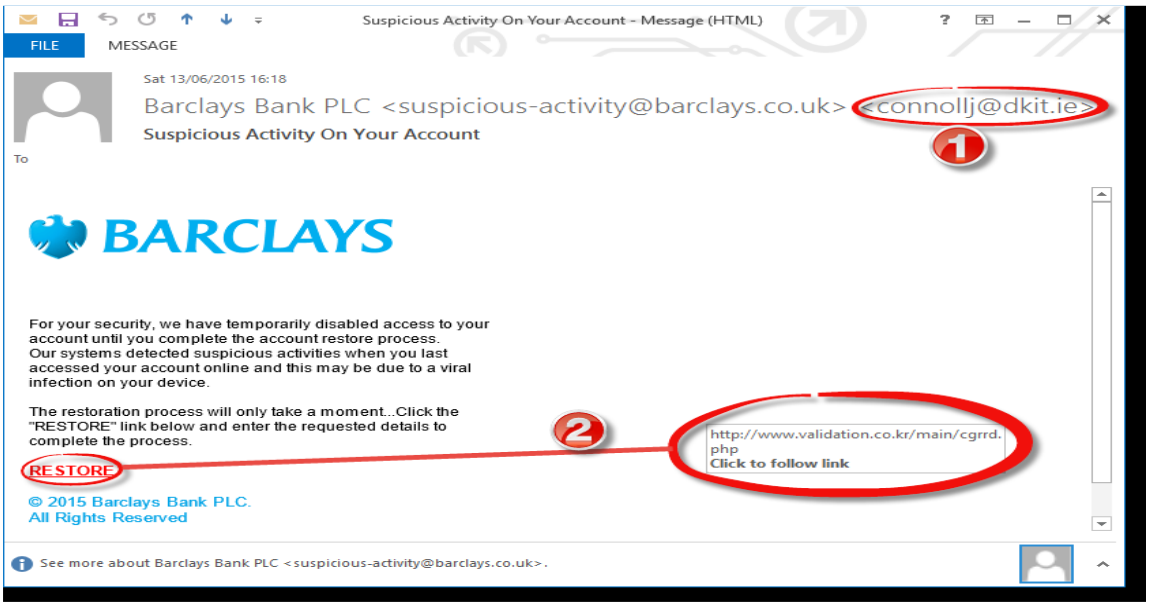
سكيرويير:

يقنع سكيرويير المستخدم بالقيام بعملية محددة نتيجة لخوفهم. يزور سكيرويير النوافذ المنبثقة التي تماثل نوافذ حوار نظام التشغيل.



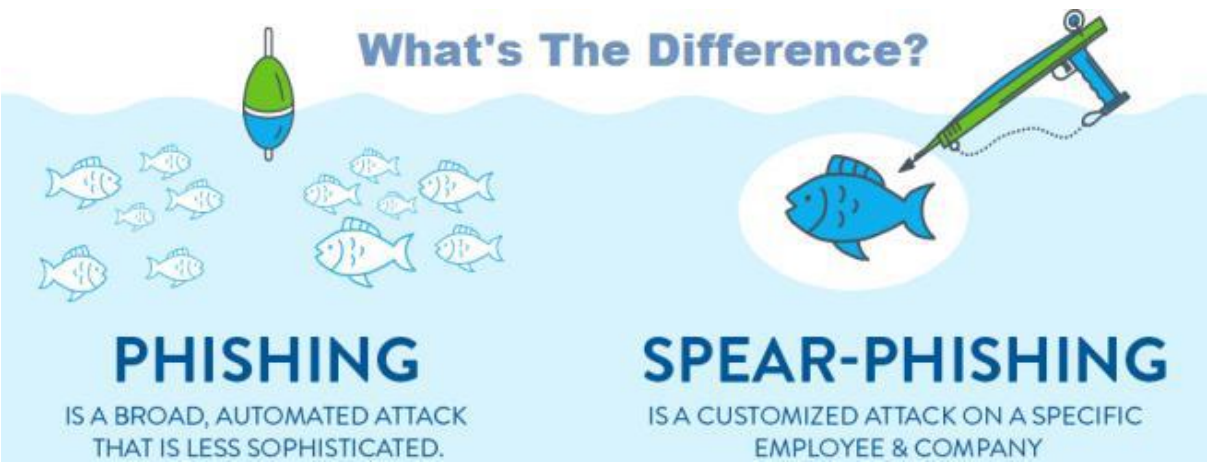
التصيد الأحتيالي:

التصيد الاحتيالي هو شكل من أشكال الاحتيال يستخدم مجرمي الأنترنت الرسائل الفورية ووسائل التواصل الاجتماعي الأخرى لمحاولة جمع معلومات مثل تسجيل الدخول إلى الشبكة أو معلومات الحساب عن طريق طريقة تنكرية كهيئة أو شخص مرموق. يحدث التصيد الاحتيالي عندما يرسل طرف مخادع بريد إلكتروني احتيالي متنكر ككونه من مصدر قانوني موثوق فيه. تهدف هذه الرسالة إلى خداع المستلم إلى تثبيت برنامج ضار على الجاز الخاص به.



تغيرات التصيد الاحتيالي:

تصيد احتيالي موجّه التصيد الاحتيالي الموجة هو هجوم تصيد احتيالي مستهدف. بينما كلا من التصيد الاحتيالي والتصيد الاحتيالي الموجهة يستخدمون البريد الإلكتروني للوصول إلى الضحايا يرسل التصيد الاحتيالي الموجهة رسائل البريد الإلكتروني المخصص إلى شخص محدد.

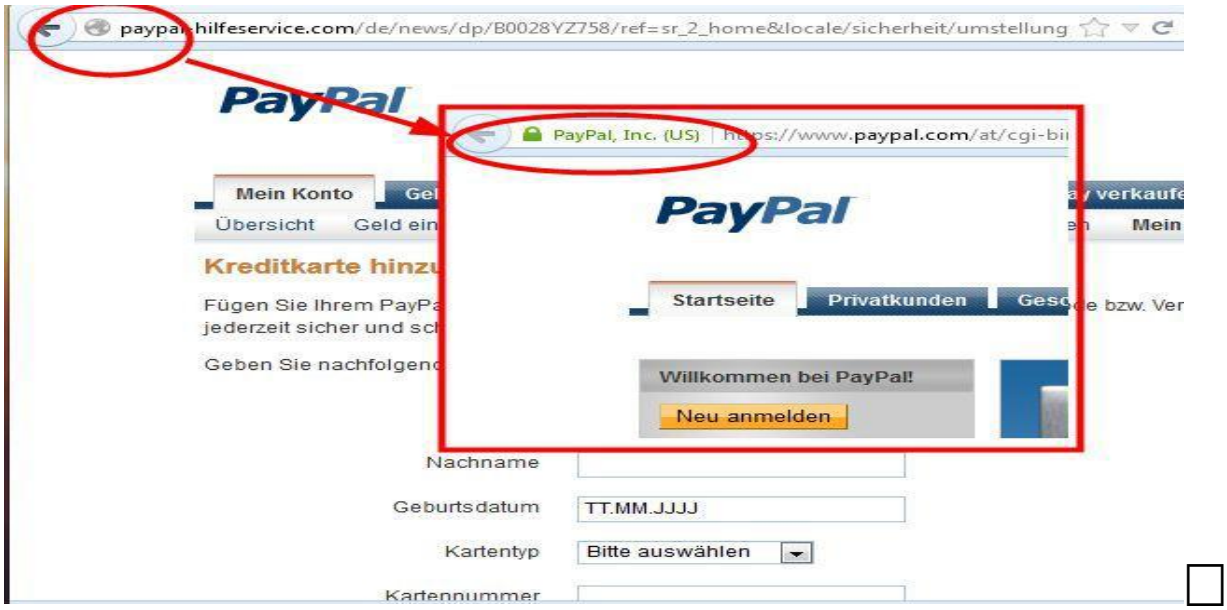


التصيد الاحتيالي عبر الأنظمة التليفونية التصيد الاحتيالي عبر الأنظمة التليفونية هو التصيد الاحتيالي باستخدام الصوت.تكنولوجيا الاتصالات. يقوم المجرمون بمكالمات احتيال عن طريق مصادر قانونية باستخدام تكنولوجيا نقل الصوت عبر بروتوكول الإنترنت. كما قد يستلم الضحايا رسالة مسجلة قد تبدو وكأنها **قانونية**.

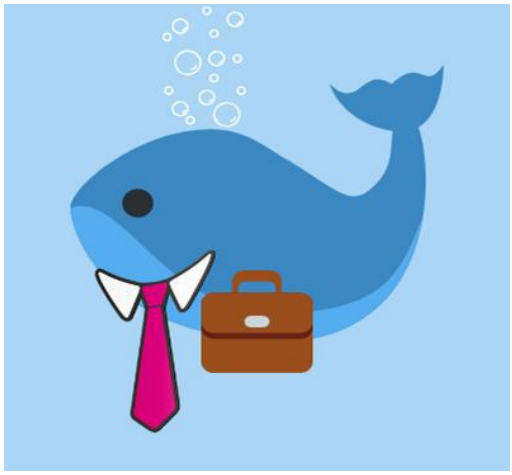
الاحتيال عبر الرسائل النصية القصيرة الاحتيال عبر الرسائل النصية القصيرة هو هجمات أمنية حيث

ينخدع المستخدم لكي يقوم بتحميل حصان طروادة أو فيروس أو برامج ضارة أخري إلى هاتفة المحمول أو جهاز محمول أخر. الاحتيال عبر الرسائل النصية القصيرة هو اختصار لكلمة التصيد الاحتيالي عبر الرسائل النصية القصيرة.

فارمينج الفارمينج هي تقمس الموقع الإلكتروني القانوني في محاولة لخداع المستخدمين إلى إدخال بيانات اعتماد الخاصة بهم.

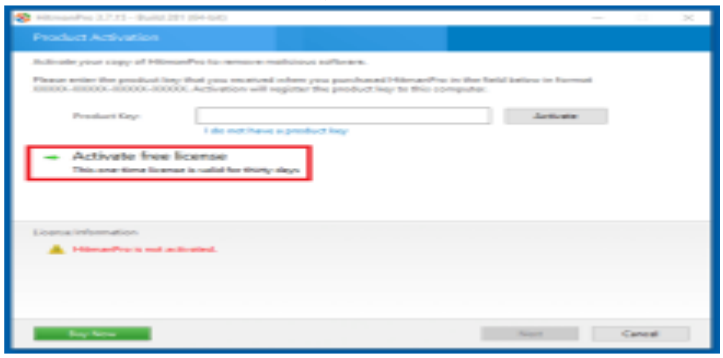


صيد الحيتان صيد الحيتان هو نوع من أنواع هجوم التصيد الاحتيالي الذي يستهدف اهداف رفيعة المستوي في المؤسسة مثل كبار المعاونين التنفيذيين.



مختطفي المتصفح:

مختطف المتصفح هو برنامج ضار يعدل إعدادات متصفح الحاسوب لإعادة توجيه المستخدم إلى مواقع الإلكترونية اتدفع عن طريق عملاء مجرمي الأنترنت. يقوم مختطفي المتصفح عادتاً بعملية التثبيت بدون إذن المستخدم **وعادة ما تكون جزء من درايف باي داونلود.**



هجمات تسمم نتائج البحث:

تعمل محركات البحث مثل جوجل من خلال ترتيب الصفحات حسب ترتيبها وتقديم نتائج البحث ذات الصلة حسب استعلامات البحث الخاصة بالمستخدم. قد تظهر بصورة أكثر أو أقل في قائمة نتائج البحث وذلك وفقاً لصلة محتوي الموقع الإلكتروني. تحسين محرك البحث هو مجموعة من التقنيات تستخدم من أجل تحسين ترتيب المواقع الإلكترونية عن طريق محرك البحث.

بينما العديد من الشركات المتخصصة في تحسين المواقع الإلكترونية لتحسين وضعها ، يستخدم هجمات تسمم نتائج البحث تحسين محرك البحث لجعل المواقع الإلكترونية الضارة تظهر بصورة أكثر في نتائج البحث.

٢,٢ الخداع:

ثمان دقائق من البحث:

تصفح الانترنت وأجد قصة مسلية حول كيفن ميتنيك.

فن الخداع:

الهندسة الاجتماعية هي طريقه غير تقينه تماماً حيث يقوم المجرمين بجمع المعلومات حول الهدف. الهندسة الاجتماعية هو هجوم يحاول استغلال الأفراد إلى اتخاذ إجراءات أو الكشف عن معلومات سرية.

تظاهر الخداع:

وذلك عندما يتصل المهاجم بشخص ما ويكذب عليه كمحاولة للوصول إلى البيانات المتميزة. مثال على ذلك، مهاجم يتظاهر بحاجته لبيانات شخصية أو مالية من أجل تأكيد هوية المستلم.

شيء مقابل شيء:

ذلك عندما يطلب المهاجم معلومات شخصية من طرف مقابل شيء ما ، كهدية مثلا.

أنواع الخداع:

تطبيقات شولدر سيرفينج ودامبستر دايفينج

انتحال الهوية والخدع

بيجي باكينج تيل جاتينج

- عبر الانترنت والبريد الإلكتروني والخداع على شبكة
-

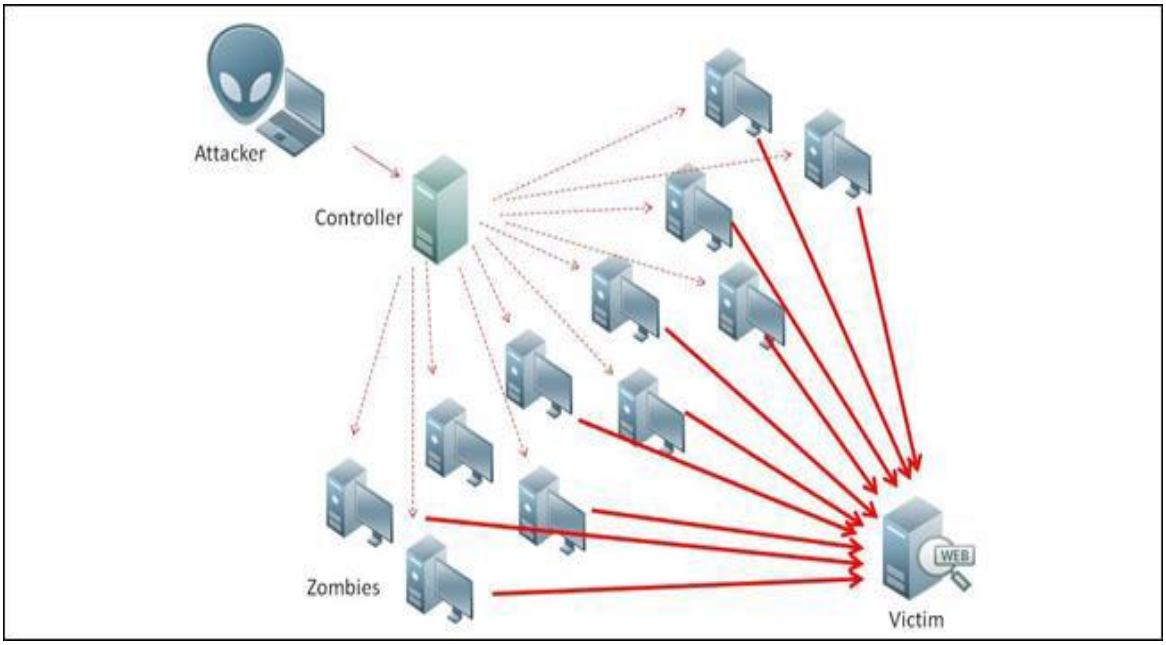
٢,٣ الهجمات

أنواع الهجمات الألكترونية:

هجمات الحرمان من الخدمات كنوع من هجوم الشبكات. يؤدي هجوم الحرمان من الشبكات في نوع ما إلى انقطاع خدمات الشبكات لأجهزة المستخدمين أو تطبيقاتهم. تُعتبر هجمات الحرمان من الخدمات مخاطرة كبيرة حيث تمكنهم من قطع الاتصال بسهولة كما تسبب خسارة فادحة في الوقت والمال. تُعتبر هذه الخدمات بسيطة نسبيا لإجراء حتى عن طريق مهاجم غير ماهر.

-

هجمات الحرمان من الخدمات الموزعة

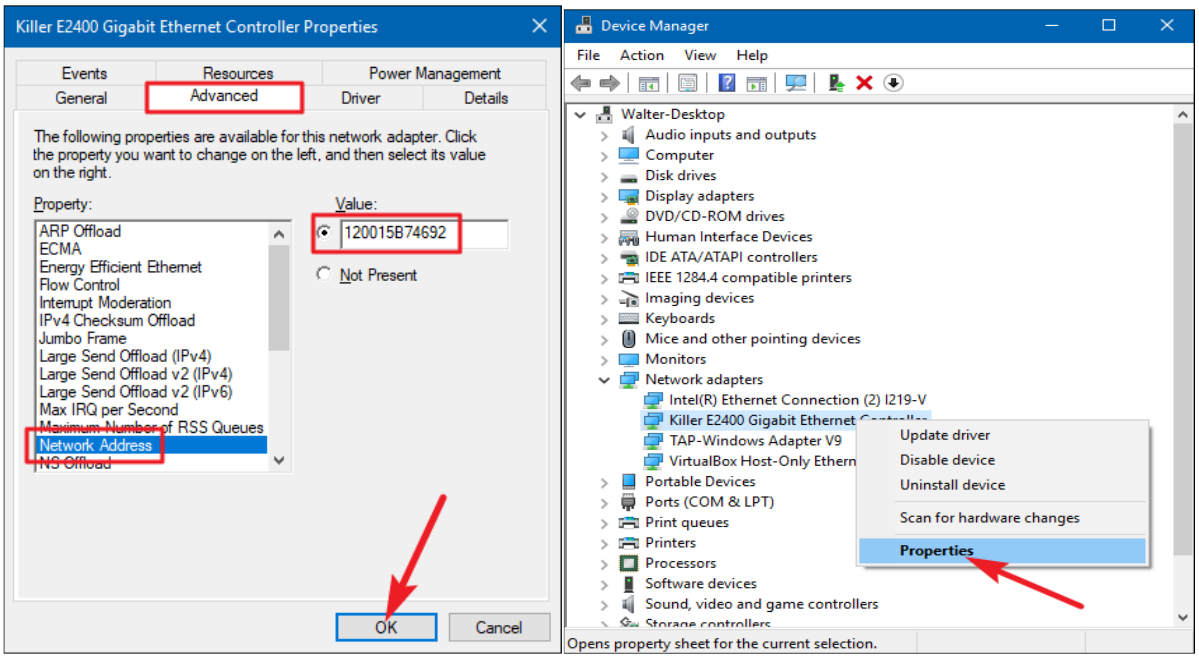


التجسس - تُعتبر عملية التجسس مشابهة تماما لعملية التنصت على شخص ما يحدث عندما يقوم المهاجم بفحص مرور الشبكة حيث تمر من خلال بطاقة الشبكة الخاصة بهم بغض النظر عما إذا كانت تلك عملية المرور موجهة إليهم أم لا. المجرمين الذين يقومون بتجسس الشبكات عن طريق تطبيق البرمجيات والأجهزة أو مزيج من الاثنين.

هجوم انتحال البريد الالكتروني انتحال البريد الإلكتروني هو الانتحال الهجوم، ويستفيد من العلاقات القامة على الثقة بين نظامين. في حال يقبل النظامين المصادقة المنجزة من قِبل

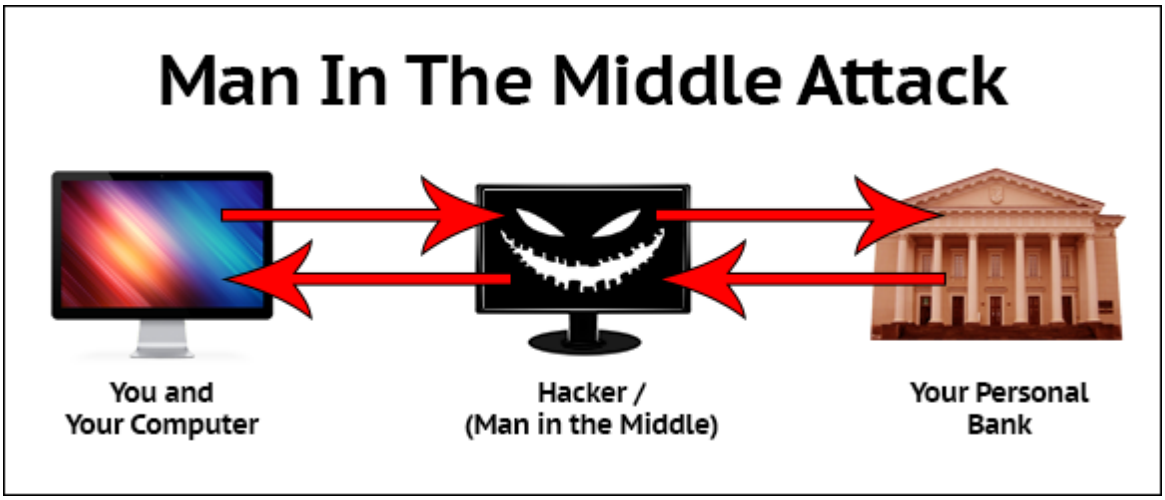
بعضهما البعض قد لا يمر الفرد الذي دخل إلى نظام واحد بعملية التصديق مرة أخرى للدخول إلى نظام آخر.

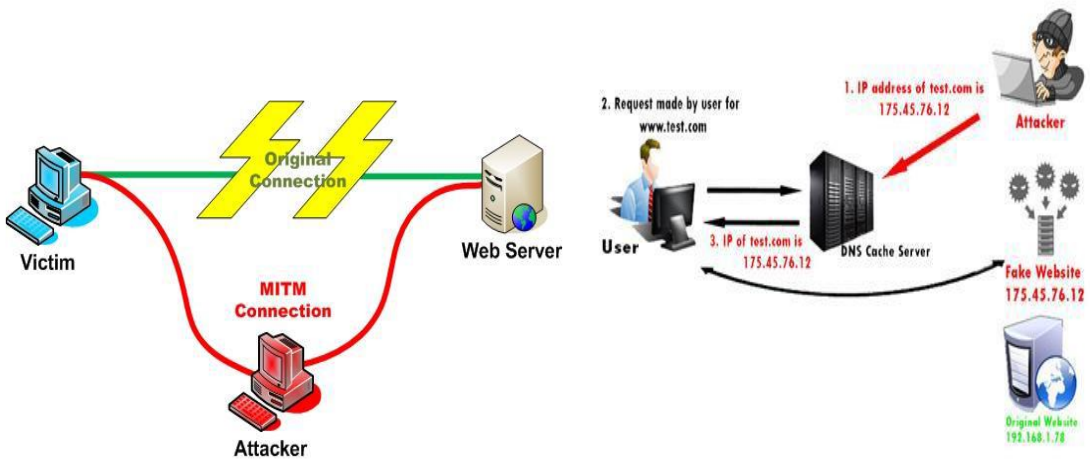
عنوان ماك لأنتحال نوافذ ويندوز



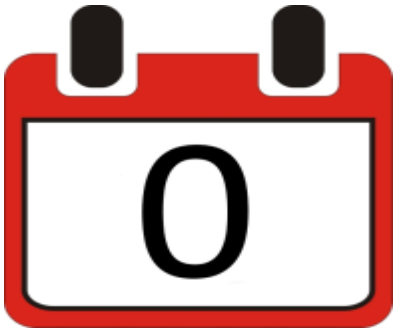
هجوم الوسيط - يقوم المجرم بالهجوم الوسيط عن طريق منع الاتصال بين أجهزة الكمبيوتر لسرقة المعلومات عبر الشبكات. يمكن للمجرم أن يقوم بالتلاعب بالرسائل ونقل معلومات خاطئة بين المضيفين وذلك لأن المضيفين ليسوا على دراية بحدوث تعديل للرسائل

- يسمح الهجوم الوسيط للمجرم بالتحكم في الجهاز بدون علم المستخدم.


Man In The Middle Attack
You and
Your Computer
Hacker /
(Man in the Middle)
Your Personal
Bank


Original Connection
Victim
Web Server
MITM
Connection
Attacker
2. Request made by user for
www.test.com
1. IP address of test.com is
175.45.76.12
Attacker
User
3. IP of test.com is
175.45.76.12
DNS Cache Server
Fake Website
175.45.76.12
Original Website
192.168.1.78

هجوم دون انتظار -يشير الهجوم دون انتظار إلى تهديد دون انتظار وهو هجوم باستخدام الحاسوب في محاولة لاستغلال ثغرات البرمجيات غير المعروفة أو غير المفصح عنها من قِبل مورد البرمجيات. يصف مصطلح ساعة الصفر اللحظة التي يكتشف فيها شخص ما استغلاله.

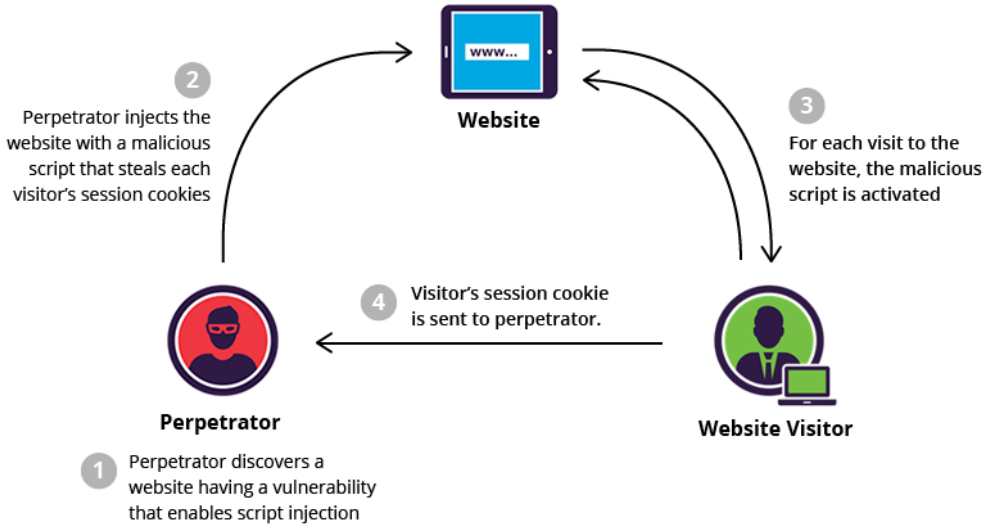


راصد لوحة المفاتيح -راصد لوحة المفاتيح هو برنامج يقوم بتسجيل أو تدوين الضغط على المفاتيح من قِبل مستخدم البرنامج. يمكن للمجرمين تنفيذ برامج ضغط المفاتيح من خلال برامج مثبتة على نظام الكمبيوتر أو من خلال الاجهزة المتصلة فعليا بجهاز الكمبيوتر. يقوم المجرم بتشكيل برنامج مسجل ضغطات لوحة المفاتيح لإرسال ملف السجل بالبريد الإلكتروني قد تقوم ضغطات المفاتيح التي تم تسجيلها في ملف السجل بكشف أسماء المستخدمين وكلمات المرور والمواقع الإلكترونية التي تم الدخول عليها والمعلومات الحساسة الأخرى.

هجمات التطبيقات:

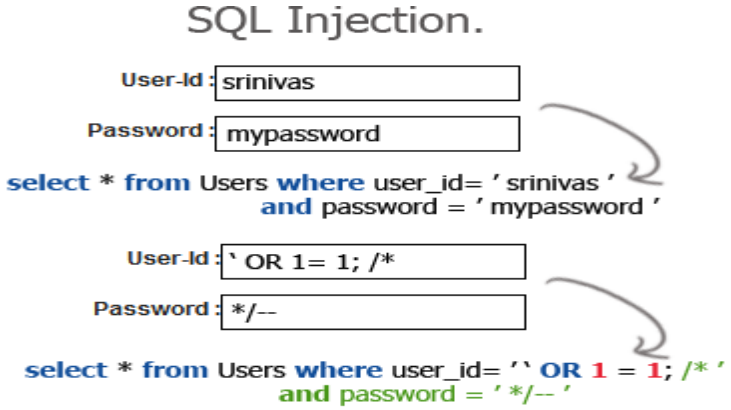
البرمجة عبر المواقع

البرمجة عبر المواقع هي نقطة ضعف موجودة في تطبيق الويب تسمح البرمجة عبر المواقع حقن نصوص من جانب العميل تشمل على برمجية ضارة في صفحات الويب المطلع عليها من قِبل الضحية. تحتوي عملية البرمجة عبر المواقع على ثلاثة مشاركين وهم: المجرم والضحية والموقع الإلكتروني. لا يستهدف المجرم الإلكتروني الضحية بصورة مباشرة ولكن يستغل نقطة الضعف داخل الموقع الإلكتروني أو تطبيق الويب.



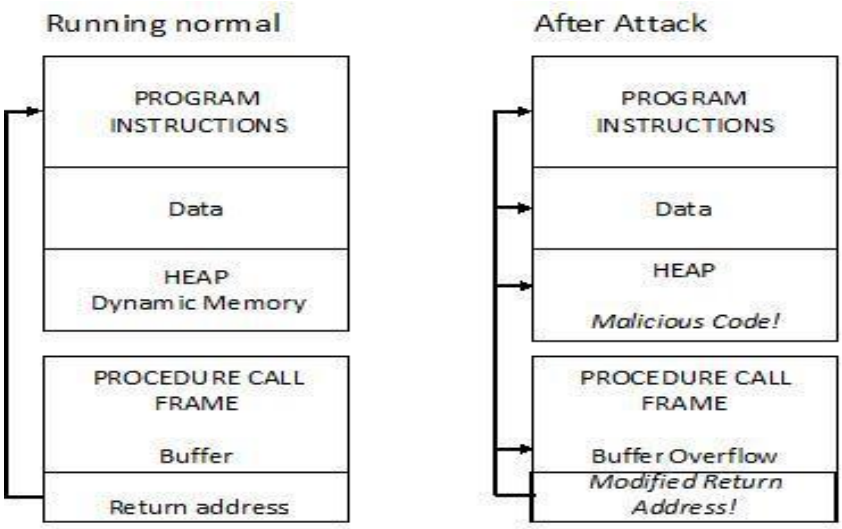
هجمات البرمجة بالحقن

يمكن استخدام قاعدة بيانات مثل قاعدة بيانات إس كيو إل (لغة الاستعلامات البنيوية) أو قاعدة بيانات لغة الترميز القابلة للامتداد من أجل تخزين البيانات بالموقع الإلكتروني بطريقة تقليدية. تستغل هجمات البرمجة بالحقن نقاط الضعف في البرنامج مثل عدم التحقق من صحة استعلامات قاعدة البيانات بصورة صحيحة.



تجاوز سعة المخزن

يحدث تجاوز سعة المخزون المؤقت عندما تتجاوز البيانات حدود المخزون المؤقت. المخازن المؤقتة هي مناطق ذاكرة مخصصة للتطبيقات. بتغيير البيانات خارج حدود المخزن المؤقت، يقوم التطبيق بالوصول إلى الذاكرة المخصصة لعمليات أخرى. يمكن أو يؤدي إلى تعطل النظام أو **اختراق البيانات أو تقديم تصاعد الامتيازات.**



Attacker plants code that overflows buffer and corrupts the return address. Instead of returning to the appropriate calling procedure, the modified return address returns control to malicious code, located elsewhere in process memory.

ضوابط التحكم آكتيف إكس وجافا

تُعتبر ضوابط التحكم آكتيف إكس جزء من البرمجيات المثبتة من قِبل المستخدم لتوفير قدرات ممتدة.

قد تكون ضوابط تحكم آكتيف إكس غير الموثوق فيها/ مجهولة ضوابط تحكم ضارة. يمكن لها مراقبة عادات التصفح أو تثبيت برامج ضارة أو تسجيل ضغطات المفاتيح. كما تعمل ضوابط تحكم آكتيف إكس في تطبيقات مايكروسوفت الأخرى.

وتعمل ضوابط تحكم جافا من خلال شارح، آلة جافا الافتراضية. تتيح آلة جافا الافتراضية وظيفة برنامج جافا. تقوم آلة جافا الافتراضية بعزل البرمجة غير الموثوق فيها من بقية نظام التشغيل. هناك نقاط ضعف تسمح للبرمجة غير المسموح بها بنشر القيود المفروضة.

ضوابط التحكم آكتيف إكس وجافا

تسمح نقاط ضعف عمليات تنفيذ المدونة البرمجية عن بعد لمجرم الانترنت في تنفيذ البرمجية الضارة بالإضافة إلى التحكم في النظام بامتيازات المستخدم الذي يقوم بتشغيل التطبيق.

يسمح تنفيذ المدونة البرمجية عن بعد للمجرم تنفيذ أي أمر على الجهاز المستهدف

مكافحة هجمات التطبيق

- قم بكتابة تعليمة برمجية صعبة
- بصرف النظر عن اللغة المستخدمة أو مصدر المدخلات الخارجية، قم بتطبيق برمجة سديدة للتعامل مع كافة المدخلات الخارجية باعتبارها عدائية .
- تحقق من صحة كافة المدخلات كما لو أنها عدائية.
- احتفظ بكافة البرمجيات بما في ذلك أنظمة التشغيل والتطبيقات المحدثة وعدم تجاهل تحديث المطالبات.
- لا يتم تحديث البرامج تلقائيا لذا على الأقل دائما .

قم بتحديد اختيار تحديث الدليل.

الملخص

تُعتبر المخاطر ونقاط الضعف والهجمات محاور أساسية للمتخصصين في الأمن الإلكتروني .

- تغطي هذه الدورة مختلف هجمات الأمن الإلكتروني التي يقوم بها مجرمي الإنترنت.
- تشرح هذه الدورة مخاطر البرامج والتعليمة البرمجية الضارة.
- تغطي الجلسة أنواع الخداع المتعلقة بالهندسة الاجتماعية. تشرح المناورة كافة أنواع الهجمات التي تجربها الشبكات السلكية واللاسلكية.
- وفي النهاية، يجري نقاش حول نقاط ضعف المقدمة في هجمات التطبيقات خلال الدورة.

ومن خلال فهم كافة أنواع المخاطر المحتملة فإن ذلك يسمح للمؤسسة تحديد نقاط الضعف التي قد تجعلها مستهدفة. يمكن للمؤسسة أن تتعلم كيفية حماية نفسها من خداع الأمن الإلكتروني والمناورات.

دورة عملية:

الحماية

تأمين الشبكة

حماية تأمين الشبكات أثناء تصميم الشبكة

- جدر الحماية
- تصفية الحزمة
- فحص الحزمة المناسبة

خوادم وكيل فحص الحزمة الشامل

- منطقة منزوعة السلاح
- أنظمة الكشف عن محاولات التدخل

الكشف عن الدخلاء بالشبكة

- يعتمد على التوقيع
- يعتمد على العيوب

- مواجهة البيانات
- شبكة خاصة أفتراضية المُبينة

أساسيات كلمة المرور

- أساسيات كلمة المرور ومبادىء فهم الحاجة الى كلمة المرور
- طول كلمة المرور
- تعقيد كلمة المرور
- إنشاء كلمة المرور وتقنيات الحفظ

التكرار

- مواجهة الكوارث
- استمرارية الاعمال
  - أمثلة المشروعات المتوقفة

الممارسة

- تعطيل الكود: هجوم عنيف، هجوم المعجم
- برنامج واير شارك

التوعية بشأن أمن المعلومات

التشفير (سري أو مخبأ)

- التشفير – فن وعلم "الأكواد السرية" وإعدادها واختراقها
- التشفير – إعداد "الأكواد السرية"
  - التشفير- فك التشفير
- تحليل الشفرات – اختراق "الأكواد السرية"
- التشفير – كل ما سبق (وأكثر)

كيف يمكنك التشفير

- تستخدم الشفرة أو نظام التشفير لترميز الرسالة غير المشفرة
- وتكون نتيجة التشفير نص مشفر
- نقوم بفك التشفير النص المشفر لاسترداد الرسالة غير المشفرة
- يستخدم المفتاح لتكوين نظام التشفير
- يستخدم المفتاح المتماثل بنظام التشفير نفسه سواء عند التشفير أو فك التشفير
- يستخدم المفتاح العام بنظام التشفير نفسه سواء عند التشفير أو فك التشفير

أفتراضات أساسية

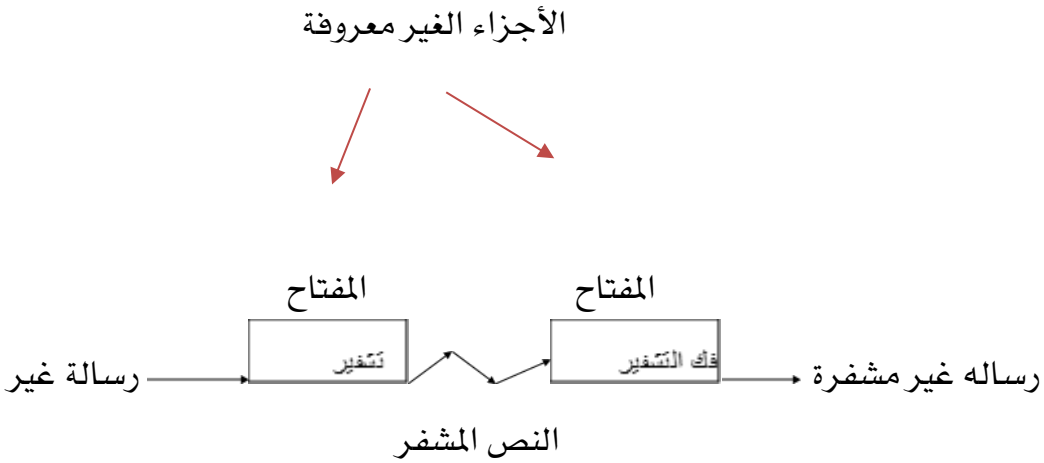
- أن النظام معروف بالكامل للمتطفل
- ويكنون المفتاح وحده سر
- ولا تكن خوارزميات التشفير سر

وتعرف بأسم مبادىء كير شوف

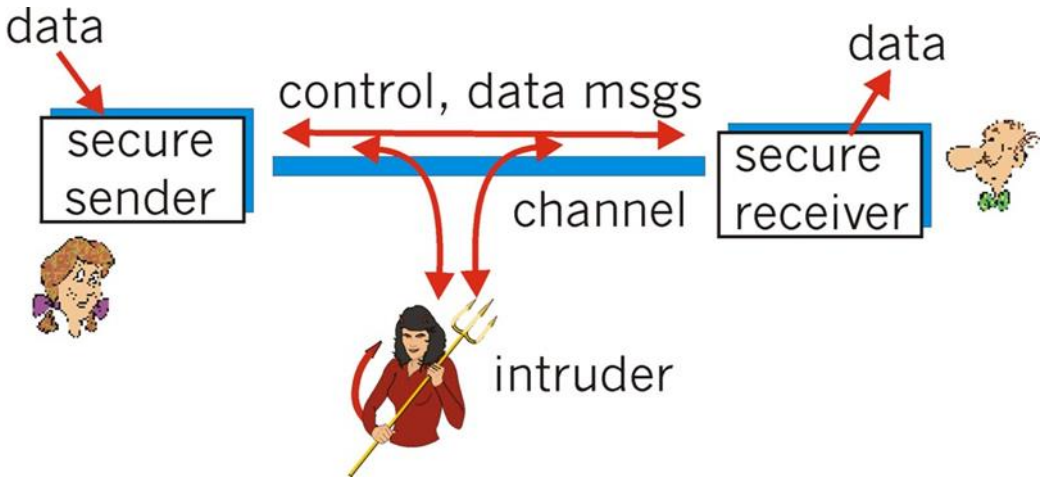
ماذا نقوم بهذا الأفتراض؟

- أظهرت الخبرة أن الخوارزميات السرية تصبح ضعيفة عند التعرض لها
- ولا تظل الخوارزميات سرية
- ومن الافضل إيجاد الضعف مُسبقاً

التشفير مثل الصندوق الأسود



الأصدقاء والأعداء: أليس وبوب وترودي



من قد يكون بوب، وأليس؟

- ...حسنًا، في أرض الواقع يكون بوب وأليس!
- متصفح الويب/ الخادم للتعاملات الإلكترونية (مثال الشراء عبر الإنترنت(
- عميل/الخادم الحساب المصرفي عبر الإنترنت
- خوادم نظام أسماء النطاقات
- تتبادل الموجهات تحديثات مسارات التوجيه
- ...

تصنيف التشفير

- المفتاح المتسق
  - نفي المفتاح للتشفيروفك التشفير
  - نوعان: عمليات تشفير التدفق، عمليات تشفير الحظر
- المفتاح العام (أو التشفير غير المتماثل)
  - مفتاحان، واحداً للتشفير (عام)، وواحد لفك التشفير (خاص)
  - أيضاً، لا يقارن أي شيء - بالتوقعات الرقمية مع تشفير المفتاح المتسق
- خوارزميات التجزئة
  - في بعض الأوقات يُنظر إلية باعتباره " أحد أساليب" التشفير

تصنيف تحليل التشفير

- من وجهة نظر المعلومات المتوفرة للمتطفل
  - النص المشفر فقط
  - نص مجرد معروف
  - نص مجرد مختار
    - "هجوم وقت الغداء"
    - قد تقوم البروتوكولات بتشفير البيانات المختارة
  - نص مجرد مختار بتكييف
  - المفتاح المتعلق
  - بحث إعادة التوجية
  - والاخرين ...

التشفير المتسق

m=رسالة النص المجرد ،

c= الشفرة (رسالة مُشفرة)

تود أليس التحويل إلى بوب سرًا
Ek(m)→c
لاحظ أن المفتاح هو نفسه بالنسبة لكلاً من بوب وأليس

الأسئلة: كيف يمكنهم تبادل المفتاح لأول مرة حيث أنهم يودون التحدث سرًا؟

يقوم بوب بتشفير (E) والرسالة بـ (m) مع المفتاح (k)

$$E_k(m) \rightarrow c$$

تقوم أليس بفك تشفير (D) وشفرة (c) للحصول على رسالة (m)

$$D_k(c) \rightarrow m, \ or \ D_k\left(E_k(m)\right) \rightarrow m$$

تصنيف المفتاح المتسق

فرة الاستبدال: استبدال شيء بآخر

شفرة الأبجدية الموحدة: استبدال حرف بالآخر حروف

الهجاء abcdefghijklmnopqrstuvwxyz :

المفتاح: ٣

الرسالة: بوب إنني أحبك النص المشفر: ere l oryh brx

السؤال: هل يمكننا فك الكود (تحليل التشفير)؟ كيف؟
- هل يتطلب الأمر هجومًا عنيفًا؟
- آخر؟

substitution cipher: substituting one thing for another

– monoalphabetic cipher: substitute one letter for another

```
plaintext:   abcdefghijklmnopqrstuvwxyz
             |                       |
ciphertext:  mnbvcxzasdfghjklpoiuytrewq
```

E.g.: Plaintext: bob. i love you. alice
ciphertext: nkn. s gktc wky. mgsbc

تشفير المفتاح الخاص

عملية التشفير المتماثل -تستخدم الخوارزميات المتماثلة-
مفتاح المشاركة المُسبقة لتشفير البيانات وفك تشفيرها، كما يُعرف الأسلوب بتشفير المفتاح الخاص. تستخدم أنظمة التشفير المتعددة التشفير المتسق. تستخدم بعضًا من مقاييس التشفير المشتركة التشفير المتسق الذي يتضمن الآتي:

- مقاييس
- خوارزم
- مقاييس تشفير البيانات

تصنيف المفتاح العام

لسؤال: كيف الموافقة على المفتاح في المقام الأول (تحديدًا إن لم يسبق لهم "الالتقاء")

في تصنيف المفتاح المتسق يشارك كلاً من الراسل والمستقبل نفس المفتاح السري.

والمشكلة الأساسية بتصنيف المفتاح السري: هي الحاجة لعمل توزيع مؤمن (تأسيس) برأس المفاتيح السرية لعمليات الإرسال قبل إرسال الرسالة نفسها.

- قدم ديفي وهيلمان نموذج جديد
- تناظر صندوق البريد:
  - قام بوب بتأمين صندوق البريد
  - تستطيع أليس إدخال حرف بالصندوق، ولكنها لم تستطع إلغاء التأمين لاستخراج رسالة البريد
  - يمتلك بوب المفتاح وبإمكانه استخراج الرسالة
- رسائل مشفرة لبوب مع مفتاحه العام
  - يستطيع التوزيع بحرية
- يقوم بوب بفك تشفير رسائله باستخدام مفتاحه الخاص
  - بوب الوحيد الذي يعلم هذا

كيف يعمل مخطط المفاتيح العامة؟ الشروط الثلاثة الأساسية:

- يجب أن يكون من السهل تشفير الرسالة ذات المفتاح الملائم أو فك تشفيرها بطريقة حسابية
- يجب أن تكون غير قابلة للتطبيق من الناحية الحسابية وذلك لاستخلاص مفتاح خاص من المفتاح العام
- يجب أن تكون غير قابلة للتطبيق من الناحية الحسابية لتحديد المفتاح الخاص من هجوم النص المجرد المختار
  - يستطيع المتطفل اختيار أي رسالة وتشفيرها والحصول على النص المشفر

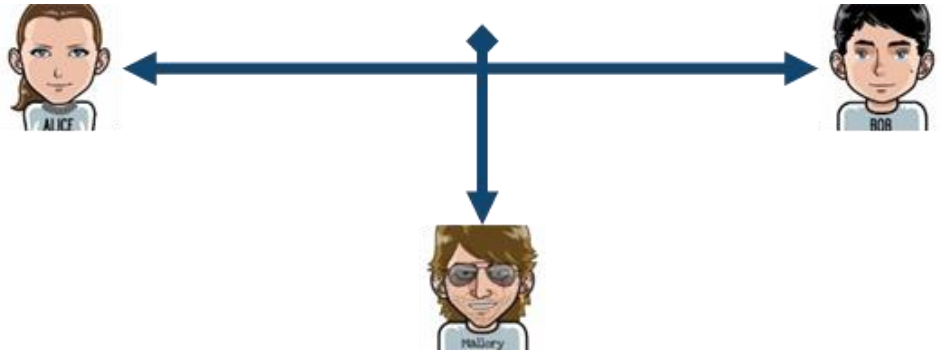
استبدال المفاتيح

يريد أليس وبوب التواصل باستخدام شفرة الكتل لتشفير رسائلهم، ولكنهم لا يمتلكون مفتاح مشاركة

كيف يحصل كلاً من أليس وبوب على مفتاح مشاركة؟

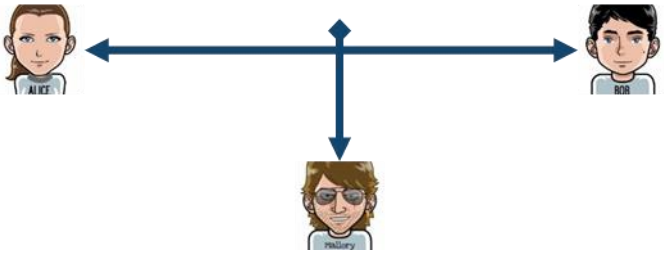
الحل الأول

- تُرسل أليس المفتاح بالإضافة إلى رسالتها المشفرة
- تطلع مالوري على الرسالة المشفرة والمفتاح
- يستخدم المفتاح لفك تشفير الرسالة



الحل الثاني

- يُرسل أليس مفتاح في وقت ما قبل إرسال بوب للرسالة المُشفرة
- يضطر مالوري أن ينتظر لوقت أطول إذا رأى تحويل المفتاح، والآن هو يمتلك
- المفتاح
- يستخدم المفتاح لفك تشفير الرسالة



الحل الثالث -استخدام تشفير المفتاح العام

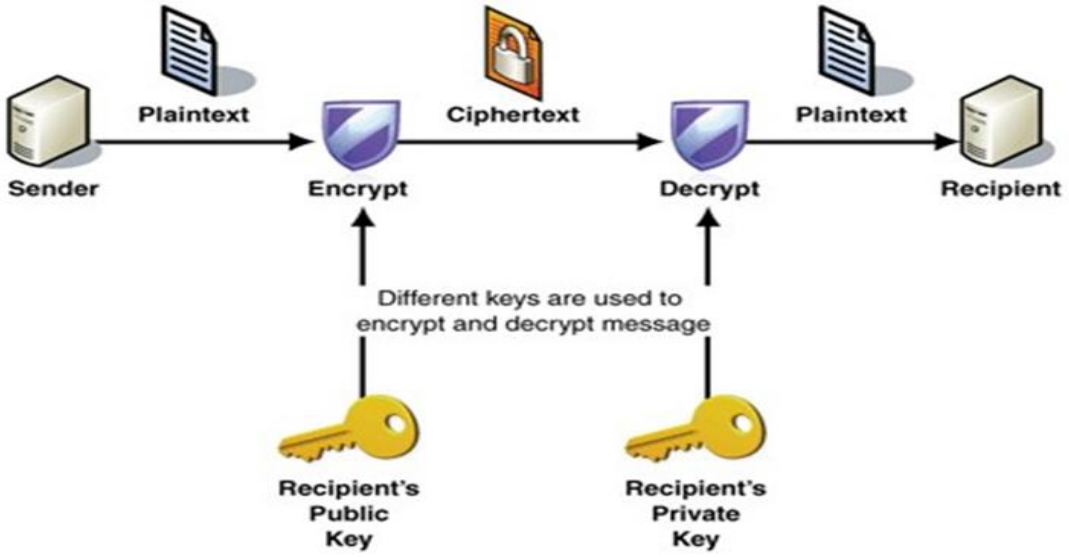
عملية تشفير المفتاح العام يستخدم المفتحان: أحدهم للتشفير الذي يختلف عن المفتاح المستخدم لفك التشفير. لا يستطيع المجرم حساب مفتاح فك التشفير المستند إلى معلومات مفتاح التشفير، والعكس، بأي فترة زمنية معقولة. تتضمن الخوارزميات غير المتماثل:

١ . تعمية بالمنحنيات الإهليجية -يستخدم المنحنيات الإهليجية كجزء من الخوارزميات. ففي الولايات المتحدة الأمريكية، تستخدم وكالة الأمن القومي الأمريكية تعمية بالمنحنيات الإهليجية لجيل التوقيع الرقمي واستبدال المفتاح.

٢ . تشفير الجمل -تستخدم مقاييس الحكومة الأمريكية للتوقيعات الرقمية. وتمتلك هذه الخوارزميات حرية الاستخدام لأن لا أحد يحمل الامتياز.

٣ . تبادل مفتاح ديفي-هيلمان -يوفر أسلوب تبادل إلكتروني لمشاركة المفتاح السري. تستخدم تبادل مفتاح ديفي-هيلمان البروتوكولات المؤمنة مثل بروتوكول طبقة المنافذ الآمنة، وبروتوكول طبقة المقابس الآمنة، وبروتوكول النقل الآمن، وحزمة بروتوكول الإنترنت الأمنية.

٤ . خوارزمية آر إس إيه -يستخدم منتج من رقمين أساسيين كبيرين ذات طول متساوي بين ١٠٠ و٢٠٠ رقم. تستخدم المتصفحات خوارزمية آر إس إيه لتأسيس الاتصال المؤمن.

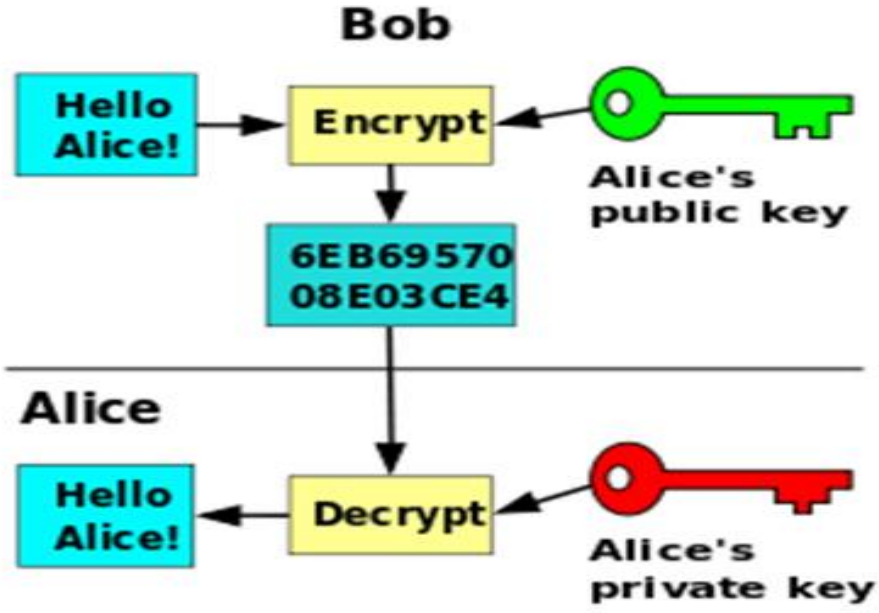


يقوم بوب بتشفير (E) والرسالة بـ (m) مع مفتاح أليس العام

$$E_{Pu_A}(m) \rightarrow c$$

تقوم أليس بفك تشفير (D) وشفرة (c) للحصول على رسالة (m)

$$D_{\Pr_A}(c) \rightarrow m, \ or \ D_{\Pr_A}\left(E_{Pu_A}(m)\right) \rightarrow m$$



- تبادل مفتاح ديفي-هيلمان

- $g \neq 0, g \neq 1$, and $g \neq p-1$
- تختار أليس مفتاحها الخاص kA
  - يقوم حساب KA = gkA بتعديل p ويُرسلها إلى بوب بالتحديد
- يختار بوب مفتاحه الخاص kB
  - حساب B=9KB تعادل P وإرسالها إلى أليس في الوضع السليم
- عندما أراد أن يتفق أليس وبوب على برهان مشترك، قاموا بحساب أ سر مسترك س
- تعادل SA.B=KB k p
- تعادل SBA=KA KB p

لماذا يتم استخدام المعادلات الخاصة بديفي؟

- sA,B=SA,B
- (gkA)kB mod p = (gkB)KA mod p

يعرف مالوري:

- G and p
- Ka and KB

لماذا لا يحاسب مالوري السر؟

$$S_{A,B} = K_B^{kA} \bmod p$$
$$S_{B,A} = K_A^{kB} \bmod p$$

كان هذا أول برهان لمخطط التشفير

المعادلات الصعبة

تقوم عمليات التشفير الرئيسية العامة على المشاكل الصعبة

تقوم معدلات ديفي-هيلمان على مشاكل لوغاريتمات المنفصلة المقدمة :

- مجموعة المضاعفةG
- عنصر a in G
- ايجاد الناتجb
- الحل الفريد لax = b in G
- xلوغلb

❖لا توجد خوارزمية متعددة الحدود لحل هذه المسالة

*On classical computers

المقارنة المتماثلة لفك التشفير الأساسي العام

الأداة الأساسية يعتبر التشفير هو أكثر كفاءة في حماية سرية الصغيرة البيانات وحجمها وسرعتها يجعلها أكثر أمانًا لمهام مثل تبادل الأدوات الإلكترونية وهي كمية صغيرة من البيانات بدلاً من تشفير كتل كبيرة من البيانات.

متماثل تعتبر أنظمة فك التشفير أكثر فعالية ويمكن التعامل معها المزيد من البيانات وعلى الرغم من ذلك، الإدارة الأساسية لأنظمة فك التشفير تعتبر الأكثر تعقيداً ويصعب التعامل معها.

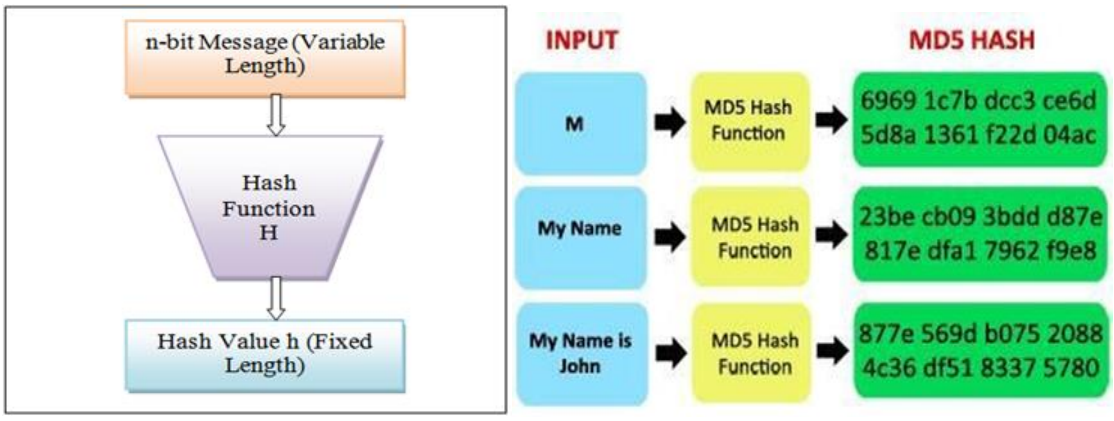
استخدامات التشفير الرئيسي العام

- السرية
  - نقل البيانات عبر قناة غير آمنة
  - تخزين آمن على وسائط إعلام غير أمنه
- المصادقة (في وقت لاحق)
- توفر التوقيعات الرقمية النزاهة وعدم التنصل
  - لا يوجد مفاتيح متماثلة لعد التنصل

دالات تجزئة

وتسمي أيضاً: الأبواب السرية، دالة ذات اتجاه واحد

التجزئة أداة تضمن نزاهة البيانات عن طريق أخذ بيانات ثنائية (الرسالة) وتقديم أطوال ثابتة وتمثيل يسمي قيمة تجزئة أو تشفير الرسالة.



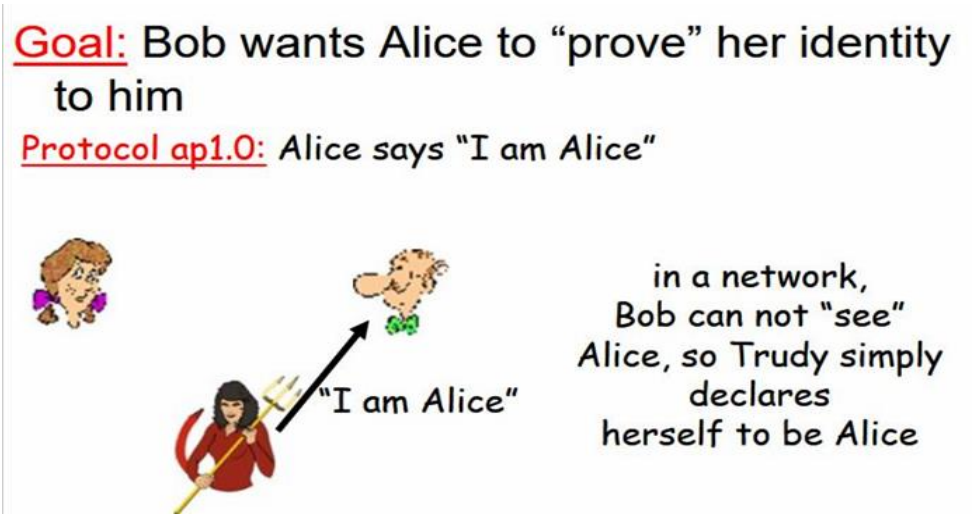
خوارزميات التجزئة

تعتبر التجزئة دالة ذات اتجاه واحد التي من اليسير نسبياً أن يتم محاسبتها ولكن يصعب بدرجة كبيرة عكسها. يعتبر طحن حبوب القهوة قياس جيد لدالة ذات اتجاه واحد. من السهل طحن حبوب القهوة، ولكن من المستحيل أن تعيد هذه القطع الصغيرة مرة آخري أو تعيدها إلى أصلها .

تتميز دالة التجزئة التشفيرية بالخصائص التالية :

- من الممكن أن تكون المدخلات طويلة .
- تحتوي المدخلات على طول ثابت .
- تعتبر دالة التجزئة ذات اتجاه واحد ولا يكمن عكسها .
- أثنين من قيم المدخلات سوف ينتج قيم تجزئة مختلفة.
- يوجد العديد من خوارزميات التجزئة الحديثة تُستخدم على نطاق واسع اليوم. وأشهر أثنين من هذه الخوارزميات هي MD5 و.SHA
- خوارزمية (MD5) تشفير الرسالة هي خوارزمية تجزئة طورها رون ريفست التي تنتج قيمة تجزئة ١٢٨ بايت .
- – (SHA)خوارزمية تجزئة أمنة التي طورها المعهد الأمريكي الوطني للمعايير والتقنية، ويمكن تنفيذها في أطوال مختلفة :
  - SHA- 224 (٢٢٤ بايت)
  - SHA- 256 (٢٥٦ بايت)
  - SHA- 384 (٣٨٤ بايت)
  - SHA- 512 (٥١٢ بايت)

المصادقة



- يكتب بوب رسالة إليّ ويحسب تشفير الرسالة (أو التوقيع)

$$h(m_1) \rightarrow s_1$$

- يُشفر بوب التوقيع عن طريق المفتاح الخاص به

$$E_{\mathrm{Pr}_B}(\mathrm{s}_1) \rightarrow \mathrm{S}$$

- يرسل بوب رسالة (إشعار بإتاحة الرسالة لكل فرد) بالإضافة إلى توقيعه

$$[m, S]$$

يمكن لأي فرد أن يستخدم المفتاح الرئيسي لكي يختبر إذا كانت الرسالة مُصدقة $[m, S]$

- يجوز لأي شخص أن يقوم بعملية الفحص، إذا صرح بوب بالآتي: $h(m') \rightarrow s'$
  - الحصول على طريقة تشفير الرسالة
  - الحصول على المفتاح الرئيسي الخاص بوب. تشفير التوقيعS الذي يقدم ملخصاً

$$D_{\mathrm{Pu}_B}(\mathrm{S}) \rightarrow s$$

إذا كان نعم، فالرسالة تعتبر مُصدقة S = S' فحص

وهذا يعنى أن ما قاله بوب صحيح للغاية والتي يقصد بها (م ١)

التوقيعات الرقمية والشهادات

التوقيعات والقانون

تقدم التوقيعات الرقمية نفس الخصائص الوظيفية مثل التوقيعات التحريرية الخاصة بالمستندات الإلكترونية .

يُستخدم التوقيع الرقمي لتحديد ما إذا قام الشخص بتعديل المستند بعد توقيع المستخدم علية .

يعتبر التوقيع الرقمي طريقة رياضية مستخدمة لفحص مصادقة ونزاهة الرسالة والمستندات الرقمية والبرمجيات .

وفى العديد من البلدان، فإن العديد من التوقيعات الرقمية لديها نفس الأهمية القانونية كما هو الحال بالنسبة للمستندات المُوقع عليها بخط اليد .

وتوفر التوقيعات الرقمية أيضاً عمليات الإنكار.

كيفية عمل تكنولوجيا التوقيع الرقمي

تعتبر عملية التشفير غير المتناظرة هي أساس التوقيعات الرقمية .

التوقيعات الرقمية:

ينتج المفتاح العمومي للخوارزميات مثل RAS مفتاحان رئيسان: مفتاح منهما خاص والآخر عام.

تعتبر المفاتيح متصلة رياضياً.

أساسيات الشهادات الرقمية

تعتبر الشهادة الرقمية بمثابة جوازات السفر الإلكترونية

تضمن الشهادات الرقمية للمستخدمين والضيوف والمنظمات لتغيير المعلومات الخاصة بهم عبر الأنترنت .

توثيق الشهادات الرقمية وتحقق بأن المستخدمين الذين يقومون بإرسال رسالة هم الأشخاص الذين يطالبون بحقهم .

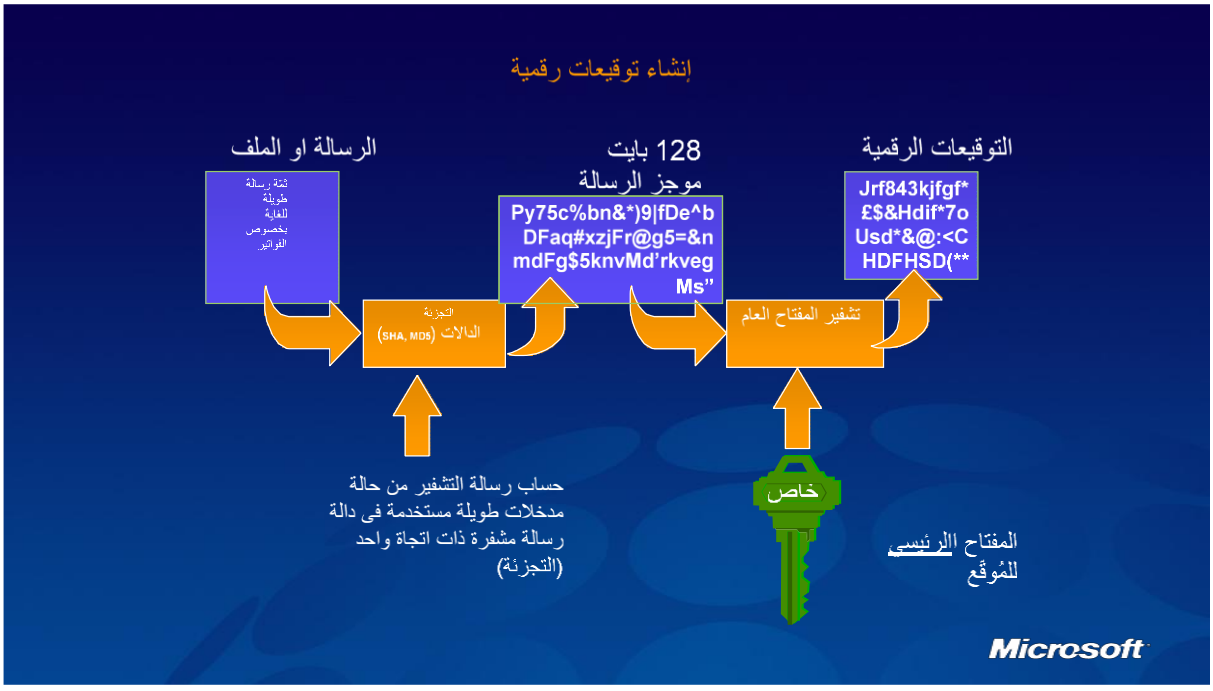
من الممكن أيضاً ان تقدم الشهادات الرقمية الطابع السري للمستخدم بالإضافة إلى الوسائل التي تعمل على تشفير أي رد.

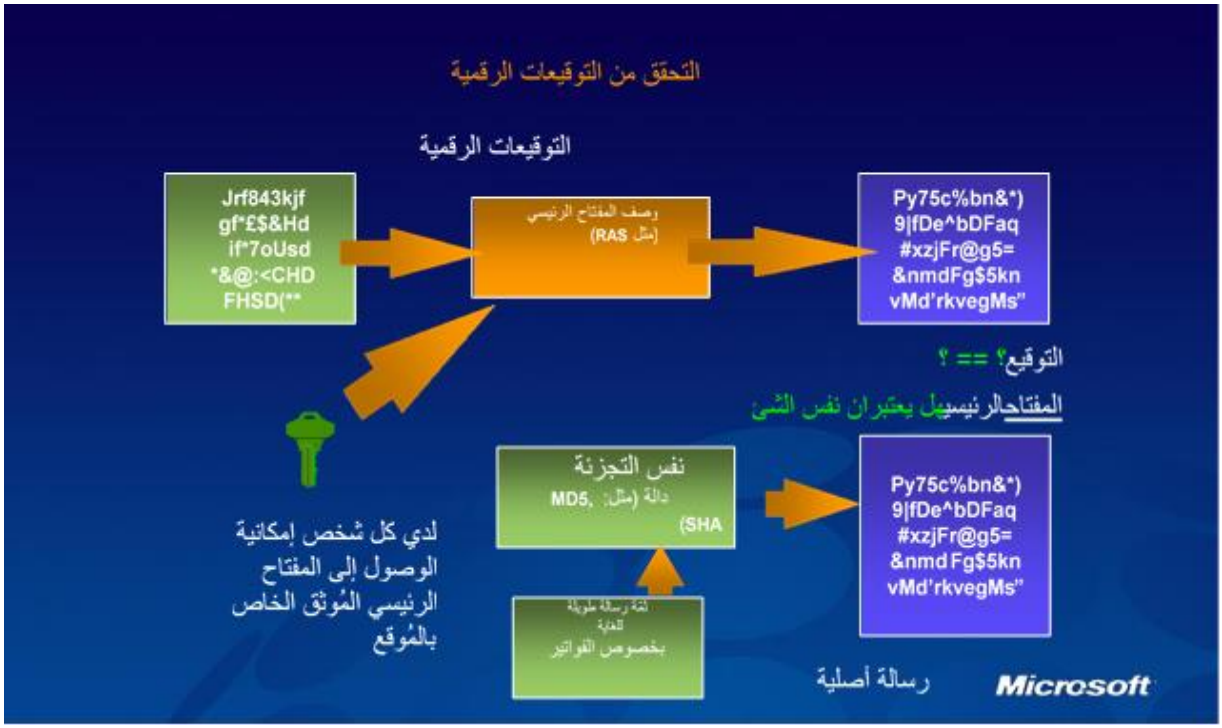
إنشاء شهادات رقمية

يجب أن تتبع الشهادات الرقمية هيكل موحد حتى يستطيع استيعاب وقراءة ذلك بغض النظر عن الجهة المُصدرة .

يعتبر X.509 هو المعيار التي يستخدم في انشاء الشهادات الرقمية والمفتاح الرئيسي للبنية التحتية الخاصة ب (PKI) المستخدم فى إدارة الشهادات الرقمية .

تعتبر PKI هي السياسات والأحكام والإجراءات اللازمة للإنشاء وإدارة وتوزيع واستخدام وتخزين وإلغاء الشهادات الرقمية.





بروتوكول طبقة الوصل الآمنة/ بروتوكول

SSL يقصد به (بروتوكول طبقة الوصل الآمنة)

- خدمة بروتوكول طبقة الوصل الآمنة
- طورت من خلال شركة نتسكيب
- صُممت النسخة رقم ٣ بمدخلات عامة
- وتصبح بعد ذلك معيار الانترنت المُعروفTLS (بروتوكول أمان طبقة النقل)
- استخدامات بروتوكول التحكم بالإرسال لتوفر خدمات كاملة يمكن الاعتماد عليها
- تحتوي طبقة الوصل الآمنة على طبقتين من البروتكولات

بروتوكول طبقة الوصل

- تُعرف شركة نتسكيب ببروتوكول طبقة الوصل الآمنة (التدفقات) ١٩٩٤
- نُشرت بروتوكول طبقة الوصل الآمنة النسخة ٢,٠ مؤخراً عام ١٩٩٥

- نُفذت النسخة ٢,٠ في منتجات شركة نتسكيب في منتصف عام ١٩٩٥
- تفاوت شركة مايكروسوفت (معاهدة التعاون بشأن البراءات) عام ١٩٩٥
- نُشرت بروتوكول طبقة الوصل الآمنة النسخة ٣,٠ بنهاية عام ١٩٩٥
- نُفذت النسخة ٢,٠ في منتجات شركة نتسكيب في منتصف عام ١٩٩٥ مع تصديق العميل

بروتوكول طبقة الوصل الآمنة -أهداف التصميم

- قابلية التجديد
  - يمكن استخدام العديد من النظم الخوارزمية للشفرة
- شفافية المستخدم
- شفافية البيانات
  - كود مصادقة الرسالة
- الإرسال الأمن بين العميل ومزود الخدمة عند أدني مستوي -مستوي طبقة الوصل
  - مواقع البروتوكول الخاص بروتوكول التحكم بالإرسال
- التحقق من هوية الأطراف الأخرى
  - يُتحقق مزود الخدمة بطريقة أتوماتيكية ويعتبر العميل في خيار من ذلك
- مستوي الكفاءة
  - التخزين المؤقت للدورات

بروتوكول طبقة الوصل الآمنة -مراجعة البروتوكول

- بروتوكول طبقة الوصل الآمنة يعتبر بروتوكول ذات طبقة متعددة المستويات
- يستلم بروتوكول طبقة الوصل الآمنة رسالة بنقل أجزاء البيانات إلى مجموعات قابلة للإدارة وضغط البيانات بطريقة اختيارية وتطبيق ماك والشفرات ونقل النتائج
- تشفير البيانات المُستلمة وضغطها والتحقق منها
- وإعادة تجميعها وتسليمها بمستوي عالي إلى العملاء
- التواصل مع البورت ٤٤٣ بشكل تلقائي
- مهلة تخزين مؤقت لتحديد هوية الجلسة بقيمة ١٠٠ ثانية

HTTPS بروتوكول نقل النص التشعبي الآمن

- امتداد بروتوكول نقل النص التشعبي الآمن لتأمين التواصل عبر الشبكة الحاسوبية
- مُستخدم على نطاق واسع على شبكة الأنترنت
- في بروتوكول نقل النص التشعبي الآمن، يُشفر بروتوكول التواصل عن طريق استخدام (بروتوكول طبقة الوصل الآمنة/ بروتوكول أمان طبقة النقل)
- وغالباً ما يُشير البروتوكول إلى بروتوكول نقل النص التشعبي الآمن عبر
- بروتوكول طبقة الوصل الآمنة، أو بروتوكول نقل النص التشعبي الآمن عبر بروتوكول أمان طبقة النقل

عن طريق استخدام بروتوكول نقل النص التشعبي الآمن يوافق الحواسب الآلية " على كود "بينهم وحينئذ يعملوا على التشويش على الرسائل المستخدمة لهذا الكود لذلك لا يستطيع أحد قراءتهم. وهذا يجعل معلوماتهم أكثر أماناً من المخترقين .

عن طريق استخدام بروتوكول نقل النص التشعبي الآمن، إذا استطاع أي شخص بين المُرسل والمستلم أن يفتح الرسائل، فأنهم مازالوا لا يستوعبون ذلك. يستطيع فقط المُرسل والمُستلم الذين هم على معرفة "بالكود"، فك تشفير الرسالة.

مزايا استخدام بروتوكول نقل النص التشعبي الآمن

- مصادقة الموقع الإلكتروني الذي يمكن الوصول اليه.
- حماية خصوصية ونزاهة البيانات المتغيرة عند عملية الإرسال
- الحماية ضد منتصف هجمات الشخص