معهد العراب العالي للتدريب

أمن أنظمة التشغيل

م. ميسون الرحماني

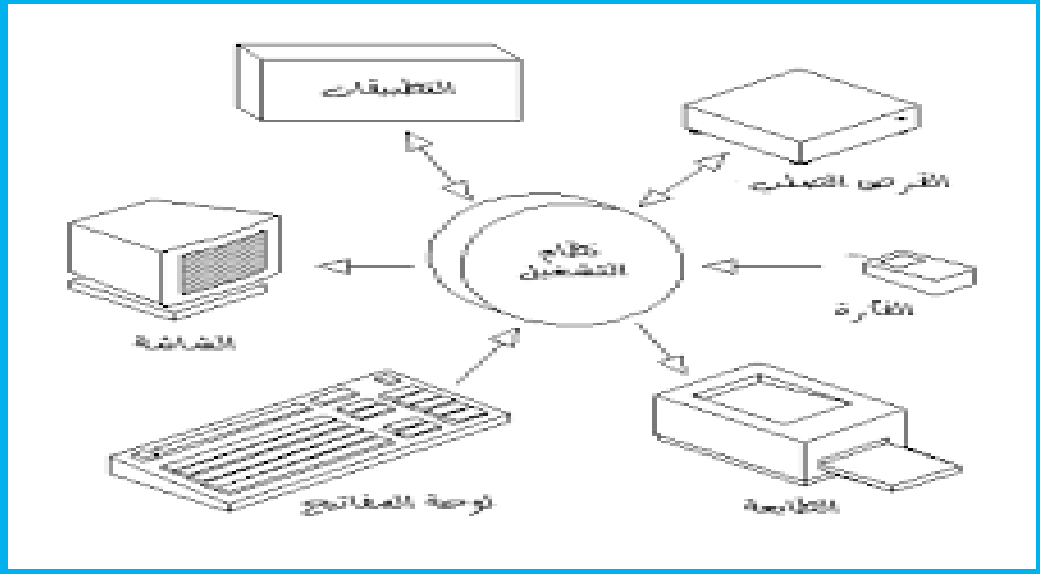
مفهوم نظام التشغيل

نظام التشغيل هو أهم البرامج التي يتم تشغيلها على جهاز كمبيوتر. فهو يدير كل ما يتعلق بذاكرة الكمبيوتر والعمليات التي تتم به ، وكذلك كل من البرمجيات والمكونات المادية (السوفتوير والهاردوير). كما أنه يتيح لك التواصل مع جهاز الكمبيوتر من دون معرفة كيفية التحدث بلغة الكمبيوتر.

مهام نظام التشغيل

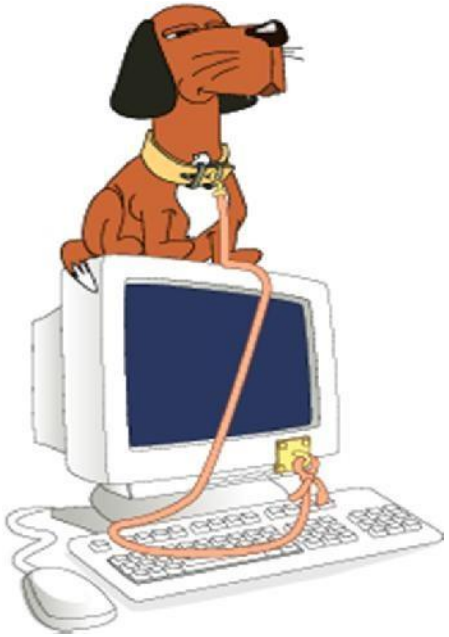
- إدارة **نظام** المدخلات والمخرجات
- إدارة العمليات
- إدارة الملفات
- إدارة وحدة الذاكرة الرئيسية
- إدارة التخزين الثانوية

أساسيات نظام التشغيل



مفهوم امن نظم التشغيل

1 المصادقة: التأكد من أن المستخدمين المصرح لهم فقط هم من يمكنهم الوصول إلى النظام.
2. التحكم في الوصول: تقييد وصول المستخدم إلى المعلومات والموارد الضرورية فقط. 3. التشفير: حماية البيانات الحساسة عن طريق تشفيرها أثناء النقل وأثناء الراحة.
4. سلامة البيانات: الحفاظ على دقة واتساق البيانات المخزنة في النظام.
5. التحقق من صحة الإدخال: التحقق من صحة إدخال المستخدم لمنع التعليمات البرمجية الضارة أو الوصول غير المصرح به.
6. معالجة الأخطاء: معالجة الأخطاء والاستثناءات والتخفيف منها لضمان استقرار النظام.
7. مسارات التدقيق: تسجيل وتتبع نشاط المستخدم لتحليل الطب الشرعي والتحقيقات الأمنية.
8. أمن الشبكات: تأمين قنوات الاتصال والبنية التحتية للشبكة من التهديدات الخارجية.
9. التحديثات والتصحيحات المنتظمة: إبقاء النظام محدثًا بأحدث الإصلاحات والتحديثات الأمنية.
10. وعي المستخدم وتدريبه: تثقيف المستخدمين حول أفضل الممارسات الأمنية وكيفية تحديد التهديدات المحتملة والإبلاغ عنها.

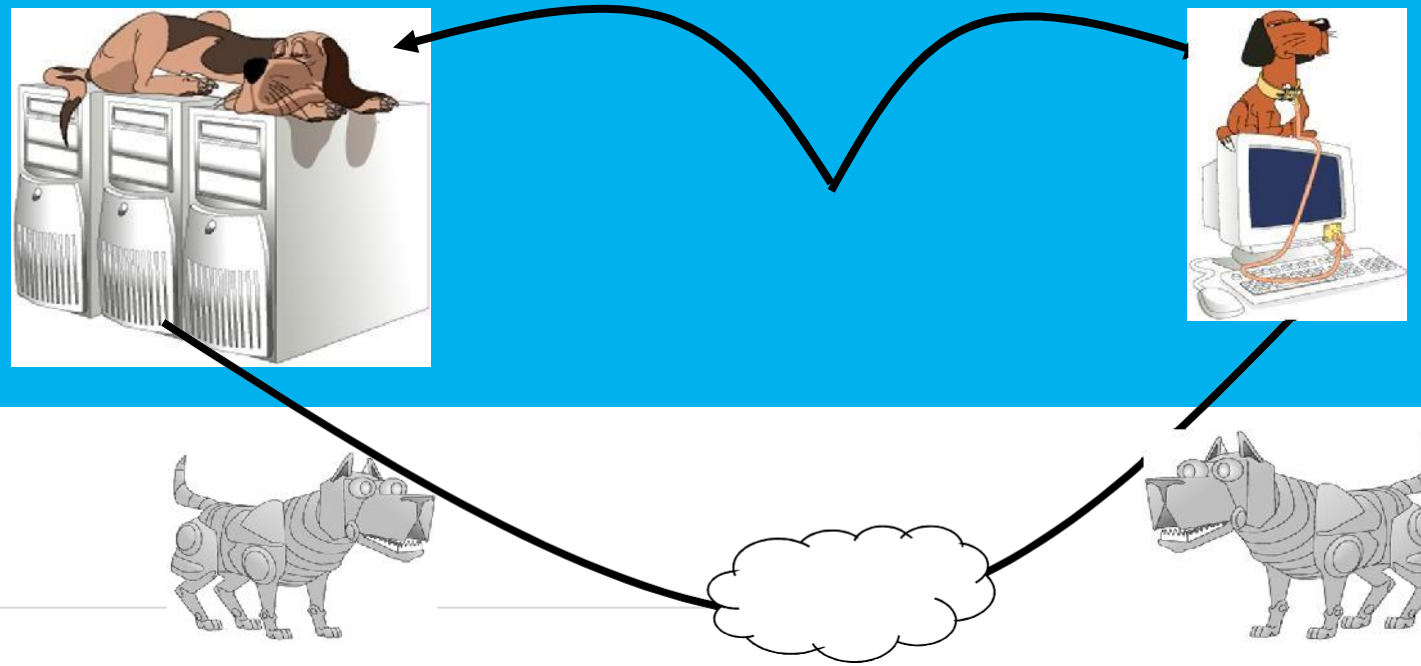


يتعلق أمن الكمبيوتر بالأحكام والسياسات المعتمدة لحماية المعلومات والممتلكات من

السرقة أو الفساد أو الكوارث الطبيعية

- مع السماح للمعلومات والممتلكات بالبقاء في متناول المستخدمين المستهدفين وإنتاجيتهم
- أمن أجهزة الكمبيوتر ضد المتسللين (مثل المتسللين) والبرامج الضارة

من ناحية أخرى، يتعامل أمن الشبكات مع الأحكام والسياسات المعتمدة لمنع ومراقبة الوصول غير المصرح به أو سوء الاستخدام أو التعديل أو الحرمان من شبكة الكمبيوتر والموارد التي يمكن الوصول إليها عبر الشبكة.



الأمان في أنظمة التشغيل ؟

يشير الأمان إلى توفير نظام حماية لموارد نظام الكمبيوتر مثل:

- وحدة المعالجة المركزية
- الذاكرة
- برامج حاسوبية والأهم من ذلك البيانات/المعلومات المخزنة في نظام الكمبيوتر.

-لذلك يجب حماية نظام الكمبيوتر ضد الوصول غير المصرح به من قبل المستخدمين و الوصول الضار إلى النظام بما في ذلك الفيروسات

Who are the attackers?

- المخربون (الهاكرز) مدفوعون بالتحدي الفكري.
- المطلعون: الموظفون أو العملاء الذين يسعون للانتقام أو الحصول على مزايا غير رسمية
- الكوارث الطبيعية: الفيضانات والحرائق والعواصف والزلازل ...
- المجرمين يسعون لتحقيق مكاسب مالية.
- الجريمة المنظمة تسعى لتحقيق مكاسب أو إخفاء الأنشطة الإجرامية.
- الجماعات الإرهابية المنظمة أو الدول القومية التي تحاول التأثير على السياسة الوطنية
- . العملاء الأجانب الذين يبحثون عن معلومات (التجسس) لأغراض اقتصادية أو سياسية أو عسكرية.

What are the vulnerabilities?

ما هي نقاط الضعف؟

نقاط الضعف المادية (على سبيل المثال، يمكن سرقة جهاز الكمبيوتر)
نقاط الضعف الطبيعية (مثل الزلازل)
نقاط الضعف في الأجهزة والبرامج (مثل الأعطال)
نقاط الضعف في الوسائط (على سبيل المثال، يمكن سرقة الأقراص الصلبة)
ثغرات الاتصال (على سبيل المثال، يمكن استغلال الأسلاك)
نقاط الضعف البشرية (مثل المطلعين) كلمات مرور تم اختيارها بشكل سيء
أخطاء البرامج (عدم موثوقية البرامج)

ميزات الأمان في نظام التشغيل

يقوم نظام التشغيل بإدارة والتحكم في الوصول إلى مكونات الأجهزة

ركزت أنظمة التشغيل على ضمان سرية البيانات

دعم أنظمة التشغيل الحديثة أربع وظائف أساسية

تحديد المستخدم بشكل إيجابي

تقييد الوصول إلى الموارد المصرح بها

سجل نشاط المستخدم

ضمان الاتصالات المناسبة مع أجهزة الكمبيوتر والأجهزة الأخرى (إرسال واستقبال البيانات)

ميزات الأمان في نظام التشغيل العادي

مصادقة المستخدمين

مقارنة كلمة المرور

حماية الذاكرة

مساحة المستخدم، الترحيل، التجزئة

التحكم في الوصول إلى الملفات وأجهزة الإدخال / الإخراج

Access control Matrix

التخصيص والتحكم في الوصول إلى الأشياء

Table Lookup

ميزات الأمان لنظام التشغيل الموثوق

تحديد الهوية والمصادقة

إلزامي (فرض أمان متعدد المستويات من خلال تصنيف البيانات والمستخدمين إلى فئات أمان مختلفة)

التحكم في الوصول التقديري (منح الامتيازات للمستخدمين)

مكافحة الفيروسات

المساءلة والتدقيق (سجل الأمان)

جدار الحماية

كشف التسلل (أنماط استخدامات النظام العادية، والشذوذات)

معهد العراب العالي للتدريب

تصلب نظام التشغيل

هي عملية تنفيذ الإجراءات الأمنية والتصحيح لأنظمة التشغيل، مثل Windowsأو Linuxأو Apple OS X، لتقويتها ضد الهجمات الإلكترونية.

تكوينات نظام التشغيل الافتراضية مخصصة لسهولة الاستخدام

يجب اتخاذ التدابير في جميع المراحل :

التثبيت Installing

التصحيح configutation

إزالة التطبيقات والخدمات والبروتوكولات غير الضرورية

برامج إضافية (مكافحة الفيروسات، وجدار الحماية، ونظام كشف التسلل، وما إلى ذلك)

اختبار الأمن

معهد العراب العالي للتدريب

شكرًا

معهد العراب العالي للتدريب

أمن أنظمة التشغيل

م. ميسون الرحماني

أنواع الهجمات الأمنية لنظام التشغيل

هجوم البرامج الضارة **Malware Attack**

مصطلح عام للبرامج ذات الأغراض الضارة

- هو برنامج يتم تضمينه أو إدراجه في النظام عن قصد لغرض ضار.
- تهدف إلى
- تسبب إزعاجًا للمستخدم
- تلف الملفات أو الأنظمة
- تعطيل وظائف الكمبيوتر والشبكة العادية

❖ **Examples**

- **Viruses, worms**
- **Logic bomb**
- **Trojan horses**
- **Spy-wares**

Name	Description
Virus	Attaches itself to a program and propagates copies of itself to other programs
Worm	Program that propagates copies of itself to other computers
Logic bomb	Triggers action when condition occurs
Trojan horse	Program that contains unexpected additional functionality
Backdoor (trapdoor)	is a secret entry point into a program that allows someone that is aware of the backdoor to gain access without going through the usual security access procedures.
Auto-rooter	Malicious hacker tools used to break into new machines remotely
Kit (virus generator)	Set of tools for generating new viruses automatically
Spammer programs	Used to send large volumes of unwanted e-mail
Flooders	Used to attack networked computer systems with a large volume of traffic to carry out a denial of service (DoS) attack
Keyloggers	Captures keystrokes on a compromised system
Zombie	Program activated on an infected machine that is activated to launch attacks on other machines
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access

Malware Attack

ممكن تقسيم البرامج الضارة إلى فئتين:

أولئك الذين يحتاجون إلى برنامج مضيف

أجزاء من البرامج التي لا يمكن أن توجد بشكل مستقل عن بعض البرامج التطبيقية الفعلية أو المرافق أو برامج النظام.

ومن الأمثلة على ذلك الفيروسات والقنابل المنطقية.Logic bomb

تلك التي هي مستقلة

هي برامج قائمة بذاتها يمكن جدولتها وتشغيلها بواسطة نظام التشغيل.

ومن الأمثلة على ذلك برامج الزومبي.و Worms

Malware Attack

الفيروسات

شيفرة خبيثة تنسخ نفسها وتخفي نفسها بداخل

برامج أخرى عادة دون علمك

الفيروس عبارة عن برنامج يمكنه "إصابة" البرامج عن طريق التعديل عليها

شبيه بالفيروس البيولوجي: يتكاثر وينتشر

يمكن أن يحدث أضرارًا جسيمة مثل مسح الملف

الديدان Worms

الدودة هي برنامج يمكنه نسخ نفسه وإرسال نسخ من كمبيوتر إلى كمبيوتر عبر اتصالات الشبكة.

دورة حياة الفيروسات

خلال حياته، يمر الفيروس النموذجي بالمراحل الأربع التالية:

مرحلة الخمول:

الفيروس خامل. سيتم تنشيط الفيروس في النهاية بسبب حدث ما، مثل تاريخ ما، أو وجود برنامج أو ملف آخر، أو تجاوز سعة القرص حدًا ما.

مرحلة الانتشار:

يقوم الفيروس بوضع نسخة مطابقة منه في برامج أخرى أو في مناطق معينة من النظام على القرص. سيحتوي كل برنامج مصاب الآن على نسخة من الفيروس، والذي سيدخل هو نفسه في مرحلة الانتشار. البيانات.

مرحلة التحفيز:

يتم تنشيط الفيروس لأداء الوظيفة المخصصة له. كما هو الحال مع المرحلة الخاملة، يمكن أن يكون سبب مرحلة التشغيل مجموعة متنوعة من أحداث النظام

مرحلة التنفيذ:

يتم تنفيذ الوظيفة. قد تكون الوظيفة غير ضارة، مثل ظهور رسالة على الشاشة، أو الضارة، مثل تدمير البرامج وملفات

أنواع الفيروسات

الفيروس الطفيلي:

الشكل التقليدي والأكثر شيوعًا للفيروسات. فيروس طفيلي يعلق نفسه على الملفات القابلة للتنفيذ وينسخ نفسه

الفيروس المقيم في الذاكرة:

يتواجد في الذاكرة الرئيسية كجزء من برنامج نظام مقيم. ومن تلك النقطة فصاعدًا، يصيب الفيروس كل برنامج يتم تنفيذه.

.

فيروس قطاع التمهيد: Boot Sector Virus

يصيب سجل التمهيد الرئيسي أو سجل التمهيد وينتشر عند تمهيد النظام من القرص الذي يحتوي على الفيروس.

فيروس التخفي:

أحد أشكال الفيروسات المصممة خصيصًا لإخفاء نفسها عن اكتشاف برامج مكافحة الفيروسات. فيروس يستخدم الضغط بحيث يكون طول البرنامج المصاب بنفس طول الإصدار غير المصاب

فيروس متعدد الأشكال:

فيروس يتحور مع كل إصابة، مما يجعل اكتشافه عن طريق "توقيع" الفيروس مستحيلاً.

الفيروس المتحول:

كما هو الحال مع الفيروس متعدد الأشكال، فإن الفيروس المتحول يتحور مع كل إصابة. الفرق هو أن: يقوم الفيروس المتحول بإعادة كتابة نفسه بالكامل عند كل تكرار، مما يزيد من صعوبة اكتشافه. تقوم الفيروسات المتحولة بتغيير سلوكها وكذلك مظهرها.

قنبلة المنطق :

القنبلة المنطقية عبارة عن كود مضمن في بعض البرامج الشرعية التي تم ضبطها على "الانفجار" عند استيفاء شروط معينة.

أمثلة على الشروط التي يمكن استخدامها كمحفزات للقنبلة المنطقية هي:

وجود أو عدم وجود ملفات معينة، يوم معين من الأسبوع أو التاريخ، أو مستخدم معين يقوم بتشغيل التطبيق

بمجرد إطلاقها، يمكن للقنبلة أن:

تغيير أو حذف البيانات أو الملفات بأكملها، تسبب في توقف الجهاز، أو القيام ببعض الأضرار الأخرى

حصان طروادة

أي برنامج ضار يسيء تفسير نفسه على أنه مفيد أو مثير للاهتمام لإقناع الضحية بتثبيته

يدعي البرنامج أن يفعل شيئا واحدا

(قد تدعي أنها لعبة) ولكنها بدلاً من ذلك تحدث ضررًا عند تشغيلها (قد تؤدي إلى مسح القرص الصلب الخاص بك).

برامج حصان طروادة لا تكرر نفسها مثل الفيروسات،

يحجز هذا البرنامج بيانات اعتماد تسجيل دخول المستخدم ويخزنها لإرسالها إلى مستخدم ضار.

سؤال و إجابة

1-المرحلة الأولي من دورة حياة الفيروسات هي .....
(الخمول-الإنتشار-التحفيز-لاشئ)

2-الفيروس الذي يصيب الذاكرة يسمي....
(الفيروس الطفيلي-فيروس الذاكرة-فيروس القطاع التمهيدي)

معهد العراب العالي للتدريب

شكرًا

معهد العراب العالي للتدريب

أمن أنظمة التشغيل

م. ميسون الرحماني

Spyware برامج التجسس

البرامج المثبتة على جهاز الكمبيوتر عادة دون علم المستخدم تقارير المعلومات مرة أخرى حول أنشطة المستخدم

يعمل البعض من خلال مراقبة ملفات تعريف الارتباط

برنامج يتجسس فعليًا على ما تفعله على جهاز الكمبيوتر الخاص بك.

على سبيل المثال:

Xeroxملفات تعريف الارتباط البسيطة، ورموز الهاتف المحمول، وبرامج زحف الويب، و

تتضمن أنواع المعلومات التي يتم جمعها مواقع الويب التي تمت زيارتها ومعلومات

جهاز الكمبيوتر الخاص بك. IPالمتصفح والنظام وعنوان

البريد العشوائي (البريد العشوائي)

ملء صناديق البريد الإلكتروني بالبريد غير المرغوب فيه.

أي شخص يستخدم البريد الإلكتروني يضمن بشكل أساسي تلقي البريد العشوائي

كيف يحصل مرسلي البريد العشوائي على بريدك؟

البحث في الويب

إرسال رسائل البريد الإلكتروني الاختبارية

تبادل أو شراء من مرسلي البريد العشوائي الآخرين

اقتراحات لتأمين جهاز الكمبيوتر/نظام التشغيل الخاص بك

1.استخدم برامج مكافحة الفيروسات.
2.اعتمادًا على نوع الجهاز، قد يحتوي برنامج مكافحة الفيروسات أيضًا على أدوات مكافحة برامج التجسس، وتصفية مكافحة البريد العشوائي، وجدار الحماية الشخصي، والمزيد
3.قم بتحديث جهاز الكمبيوتر الخاص بك بانتظام.
4.كن حذرا مع مرفقات البريد الإلكتروني
.jpg .bmp .pdf .txt : آمن
.exe .doc .xls .ppt :غير آمن
5.استخدم جدار الحماية لحمايتك من هجمات البرامج الضارة

مراقبة التهديدات

1. تحقق من وجود: كلمات مرور قصيرة أو سهلة التخمين
2. برامج غير المصرح بها البرامج غير المصرح بها في أدلة النظام
3. عمليات غير متوقعة طويلة الأمد
4. حماية غير مناسبة لملفات بيانات النظام
5. إدخالات خطيرة في مسار بحث البرنامج (حصان طروادة)
6. التغييرات في برامج النظام: مراقبة قيم المجموع الاختباري

حماية نظام التشغيل من البرامج الضارة

1. تثبيت التحديثات
2. استخدام الماسحات الضوئية للبرمجيات الخبيثة
3. النسخ الاحتياطي للأنظمة وإنشاء أقراص الإصلاح
4. إنشاء وتنفيذ السياسات التنظيمية

Windowsتثبيت التحديثات لنظام التشغيل

تحديث ويندوز يوفر الوصول إلى التصحيحات التي يتم إصدارها/إصدارها بانتظام

يوفر الوصول إلى التصحيحات التي يتم إصدارها/إصدارها بانتظام

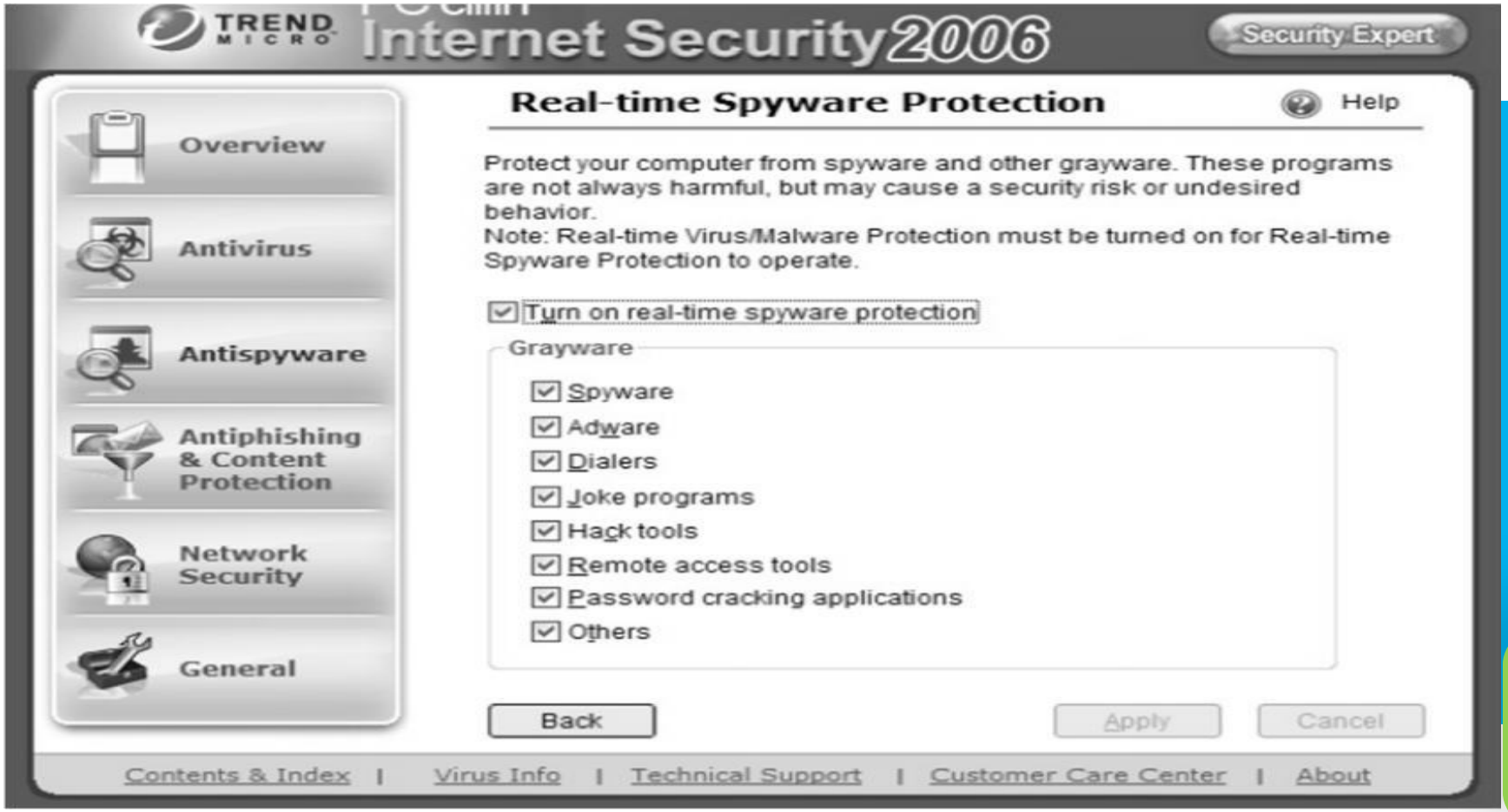
حزم الخدمة:

معالجة مشكلات الأمان والمشكلات التي تؤثر على الاستقرار أو الأداء أو تشغيل الميزات

المضمنة في نظام التشغيل

تصحيح: Patch
يعمل هذا على إصلاح شيء صغير وعادةً ما يكون سريع التنزيل والتثبيت.
التراكمي: Rollup
قد يتضمن هذا مجموعة من التصحيحات لأحد البرامج.
التحديث: Update
قد تضيف التحديثات ميزات في برنامجك أو تصلحها أو تصلح تصحيحًا سابقًا.
حزمة الخدمة: Service Pack
هذه هي المشكلة الكبيرة؛ تلك التي تقرأ عنها في الأخبار عندما تقوم Microsoftبإصدار بعض حزم الخدمات الكبيرة

Virus Scanning Software



معهد العراب العالي للتدريب

شكرًا

معهد العراب العالي للتدريب

أمن أنظمة التشغيل

م. ميسون الرحماني

التشفير والتوقيع الرقمي هما تقنيتان مهمتان في مجال الأمان السيبراني لحماية البيانات والتأكد من صحة الهوية.
إليك بعض التفاصيل حول كل منهما:

التشفير:

التشفير هو عملية تحويل البيانات من صيغة قابلة للقراءة إلى صيغة غير قابلة للقراءة أو الفهم بواسطة أشخاص غير مصرح لهم.

يتم استخدام خوارزميات التشفير لتحويل البيانات الأصلية (النص العادي) إلى شكل مشفر (النص المشفر) باستخدام مفتاح.

.

هناك نوعان رئيسيان للتشفير: التشفير متماثل والتشفير الغير متماثل

في التشفير المتماثل، يتم استخدام نفس المفتاح لتشفير وفك تشفير البيانات. يعتمد سرية البيانات على سرية المفتاح.

في التشفير الغير متماثل يتم استخدام مفتاحين متناقضين: مفتاح عام للتشفير ومفتاح خاص لفك التشفير. يعتمد سرية البيانات على سرية المفتاح الخاص

التوقيع الرقمي:

التوقيع الرقمي هو عملية تأكيد هوية مرسل البيانات وتحقق صحة البيانات المرسلة باستخدام تقنيات التشفير العام.

يتم إنشاء التوقيع الرقمي باستخدام مفتاح خاص يعود إلى المرسل، ويتم التحقق من صحته باستخدام المفتاح العام المقابل.

في العملية، يتم تطبيق خوارزمية التجزئة الرقمية (Digital Digest) على البيانات لإنتاج مجموعة تجزئة رقمية ((Digest، ثم يتم تشفير المجموعة بمفتاح خاص للمرسل لإنتاج التوقيع الرقمي.

يتم إرفاق التوقيع الرقمي مع البيانات المرسلة، ويمكن للمستلم استخدام المفتاح العام للتحقق من صحة التوقيع والتأكد من أن البيانات لم تتم تعديلها بعد التوقيع.

تستخدم التشفير والتوقيع الرقمي في العديد من المجالات، مثل:

1- حماية البيانات السرية: يتم استخدام التشفير لحماية البيانات الحساسة، مثل معلومات العملاء والمعاملات المالية عبر الإنترنت.

2- التأكد من صحة المصدر: يستخدم التوقيع الرقمي للتحقق من هوية المرسل وضمان أن البيانات لم تتم تعدل أو تتلاعب بها أطراف ثالثة.

3- التوثيق الإلكتروني: يمكن استخدام التوقيع الرقمي لتوثيق الوثائق الإلكترونية، مثل العقود والاتفاقيات، وتحقيق صحة وسلامة هذه الوثائق.

4- الأمان في الاتصالات: يمكن استخدام التشفير لتأمين الاتصالات عبر الشبكات، مثل البريد الإلكتروني والمراسلات الفورية، لحماية البيانات من الوصول غير المصرح به

استخدام التشفير والتوقيع الرقمي له أهمية كبيرة في حماية البيانات وضمان الأمان السيبراني. إليك بعض الأهميات الرئيسية لاستخدامهما:

سرية البيانات: باستخدام التشفير، يتم تحويل البيانات إلى شكل غير قابل للقراءة، ويمكن قراءتها فقط باستخدام المفتاح الصحيح. هذا يحمي البيانات الحساسة من الوصول غير المصرح به والتجسس

.

تأكيد هوية المرسل: يساعد التوقيع الرقمي في التحقق من هوية المرسل للبيانات. بفضل المفاتيح العامة والخاصة، يمكن التحقق من أن المرسل هو الشخص الحقيقي المعتمد لإرسال البيانات وأنها لم تتعرض للتلاعب.

سلامة البيانات: يُستخدم التوقيع الرقمي للتحقق من سلامة البيانات المرسلة. إذا تم تعديل البيانات بأي طريقة بعد التوقيع، فإن التوقيع سيفشل عملية التحقق، مما يشير إلى أن البيانات تمت مساومتها.

النزاهة والثقة: باستخدام التوقيع الرقمي، يتم إنشاء دليل على أن البيانات لم تتم تغييرها وأنها تمت مراقبتها من قبل المرسل. هذا يساعد على بناء الثقة بين الأطراف المعنية ويضمن النزاهة في التواصل وتبادل البيانات.

التوقيع الرقمي يعتمد على مبدأ المفاتيح العامة والخاصة والتشفير الرياضي. وسوف نوضح خطوات عمل التوقيع الرقمي والتحقق منه:

1- إنشاء المفاتيح:

يقوم المستخدم بإنشاء زوج من المفاتيح: المفتاح الخاص والمفتاح العام. المفتاح الخاص يتم الاحتفاظ به بسرية تامة، بينما يتم توزيع المفتاح العام للأطراف الأخري

2- توقيع البيانات:

يقوم المستخدم بتشفير الملخص الرقمي للبيانات المراد توقيعها باستخدام المفتاح الخاص. الملخص الرقمي هو ملخص فريد وثابت يتم استخلاصه من البيانات باستخدام خوارزمية تجزيئية مثل SHA-256.

بمجرد تشفير الملخص الرقمي بالمفتاح الخاص، يتم إنتاج التوقيع الرقمي للبيانات

التحقق من التوقيع:

يستخدم مرسل البيانات المفتاح العام للمستلم للتحقق من التوقيع الرقمي. يستخدم المرسل المفتاح العام لفك تشفير التوقيع الرقمي والحصول على الملخص الرقمي المشفر.

يستخدم المرسل الآن نفس خوارزمية تجزيئية (SHA-256) لاستخراج ملخص رقمي جديد من البيانات الأصلية.

يتم مقارنة الملخص الرقمي الجديد المستخرج مع الملخص الرقمي المشفر الذي تم فك تشفيره من التوقيع الرقمي. إذا تطابق الاثنان، فإن ذلك يشير إلى أن البيانات لم تتعرض للتلاعب وأن التوقيع صحيح

تجدر الإشارة إلى أن استخدام المفاتيح العامة والخاصة يسمح للأطراف الأخرى بالتحقق من التوقيع دون الحاجة إلى الوصول إلى المفتاح الخاص. وبالتالي، يمكن للمرسل أن يوزع مفتاحه العام ويسمح للمستلمين بالتحقق من التوقيع الرقمي الخاص به.

من خلال هذه العملية، يتم التأكد من أن البيانات لم تتعرض للتلاعب وأن المرسل هو الشخص الحقيقي للبيانات، مما يوفر الأمان والثقة في عمليات التواصل الإلكتروني.

سؤال و إجابة

معني كلمة التشفير ؟

التشفير هو عملية تحويل البيانات من صيغة قابلة للقراءة إلى صيغة غير قابلة للقراءة أو الفهم بواسطة أشخاص غير مصرح لهم.

تعد الخطوة الاولي في عملية التوقيع الرقمي هي إنشاء المفتاح .
(العبارة صحيحة أم خطأ)

عبارة صحيحة

نشاط مناقشة البحث المطروح عن أمان أنظمة التشغيل

ماهي اساسيات البحث ؟

ماذا استفدت من هذا النشاط ؟

دراسة حالة ..

معهد العراب العالي للتدريب

شكرًا

معهد العراب العالي للتدريب

أمن أنظمة التشغيل

م. ميسون الرحماني

تأمين أنظمة التشغيل التجارية يشكل تحديًا كبيرًا نظرًا للعديد من العوامل المحتملة التي يمكن أن تسبب ثغرات أمنية. فيما يلي بعض الصعوبات الشائعة التي تواجه تأمين أنظمة التشغيل التجارية:

1. ثغرات البرمجيات: يمكن أن تحتوي أنظمة التشغيل على ثغرات برمجية قابلة للاستغلال تتيح للمهاجمين الوصول غير المصرح به. قد يتم اكتشاف هذه الثغرات عندما يتم الإبلاغ عنها من قبل الباحثين في مجال الأمان، ولكن قد يتعذر اكتشاف بعضها حتى يستغلها المهاجمون.

2.
تحديثات الأمان: يتطلب تأمين نظام التشغيل النجاح الحفاظ على النظام محدثًا بأحدث التصحيحات والتحديثات الأمنية. ومع ذلك، قد يواجه المسؤولون تحديات في إدارة عملية التحديث، بما في ذلك ضمان توافق التحديثات مع التطبيقات والأجهزة الأخرى واختبارها بشكل صحيح قبل نشرها.

3.
التهديدات الجديدة: يتطور المشهد الأمني باستمرار، ويتطور المهاجمون وأساليبهم لاختراق الأنظمة. قد تواجه الشركات تهديدات جديدة ومتطورة مثل البرامج الضارة المستهدفة والهجمات السيبرانية المتقدمة، والتي يمكن أن تكون أكثر صعوبة في اكتشافها ومكافحتها.

4.
إدارة الصلاحيات: يجب أن تتم إدارة الصلاحيات بعناية لمنع وصول غير مصرح به إلى النظام. يجب أن يتم تعيين الصلاحيات بشكل صحيح للمستخدمين والمجموعات، وتقييد الوصول إلى الموارد الحساسة والضمانات الأخرى.

5.
الهجمات الداخلية: قد تحدث التهديدات الأمنية من داخل المؤسسة، سواء بشكل عمد أو غير عمد. يجب تطبيق سياسات الأمان والرقابة الداخلية المناسبة للحد من المخاطر المرتبطة بالموظفين والمستخدمين الداخليين.

6.
التوافق والتكامل: في بعض الحالات، قد يكون من الصعب تأمين أنظمة التشغيل التجارية بسبب توافقها مع تطبيقات وأجهزة أخرى. قد يتطلب التحديث إلى نظام تشغالتجارية توافقًا وتكاملًا شاملًا مع بنية الشبكة والأنظمة الأخرى في المؤسسة.

الأدوات والبرامج التي يمكن استخدامها لتحسين أمان أنظمة التشغيل التجارية

1.أدوات اختبار الاختراق (Penetration Testing Tools): تساعد هذه الأدوات في تقييم أمان النظام عن طريق تحليل الثغرات المحتملة واختبار قدرة النظام على مقاومة الهجمات. مثال على ذلك هو Metasploit.

2.
أدوات كشف الضعف (Vulnerability Scanning Tools): تستخدم هذه الأدوات لاكتشاف الثغرات الأمنية في النظام عن طريق فحص البرمجيات والتكوينات والخدمات المثبتة. مثال على ذلك هو Nessus.

3.

أدوات إدارة تهديدات الأمان (Security Threat Management Tools):تساعد هذه الأدوات في رصد وتحليل التهديدات الأمنية والاستجابة لها. تقدم هذه الأدوات إشعارات في الوقت الحقيقي عن الأنشطة الغير مشروعة وتساعد في تحليل السجلات الأمنية. مثال على ذلك هو Splunk.

4.
أدوات إدارة الصلاحيات (Access Management Tools): تساعد في إدارة ومراقبة الصلاحيات والوصول إلى النظام. تسمح هذه الأدوات بتعيين صلاحيات محددة للمستخدمين وفرض سياسات الوصول. مثال على ذلك هو Active Directory من مايكروسوفت.

الاختلافات بين هذه الأدوات ومساعدتك في اختيار الأداة المناسبة لمؤسستك

هنا بعض العناصر التي يجب مراعاتها عند اختيار أداة لتحسين أمان أنظمة التشغيل

1. المتطلبات والاحتياجات الفردية: قبل اختيار أي أداة، يجب أن تحدد المتطلبات الفردية لمؤسستك بشكل واضح. ما هي الثغرات الأمنية المحتملة التي تحتاج إلى حلها؟ ما هي الوظائف الأساسية التي تبحث عنها في الأداة؟ ينبغي أن تكون الأداة قادرة على تلبية احتياجاتك الفردية.

2.
الميزانية: يجب أن تأخذ في الاعتبار الميزانية المتاحة لديك. قد تكون بعض الأدوات مكلفة جدًا، في حين أن البعض الآخر قد يكون أكثر تناسبًا مع ميزانيتك. قم بتقييم تكلفة الأداة بالنسبة لقيمتها المضافة وقدرتها على تلبية احتياجاتك.

سؤال و إجابة

مناقشة عن صعوبات واجهة شركات
علي أرض الوقع

معهد العراب العالي للتدريب

شكرًا