Chapter 10: Security and protection

Security and protection Introduction الأمن والحماية مقدمة

- Protection refers to a mechanism for controlling the access of programs, processes or users to the resources.
- الحماية:- تشير الى آلية للتحكم في وصول البرامج ، العمليات أو المستخدمين الى الموارد.
- Security is a measure of confidence that the integrity of a system and its data will be preserved.
- الأمن :- هو مقياس للثقة بأن سلامة النظام وبياناته سيتم الحفاظ عليها.

Security and protection Goals of protection الأمن والحماية أهداف الحماية

Reasons for protection أسباب الحماية

- Prevent the mischievous, intentional violation of an access restriction
- منع الانتهاك المتعمد المؤذي لقيد الوصول.
- Ensure that each program component uses system resources only in ways consistent with system policies.
- ضمان أن كل مكون برنامج يستخدم موارد النظام فقط بطرق تتفق مع سياسات النظام.

Security and protection Principles of protection مبادئ الحماية

- A key principle for protection is the principle of least privilege.
- مبدأ اساسي للحماية هو مبدأ الامتيازات الأقل.
- Programs, users and systems are given just enough privileges to perform their tasks.
- يتم منح البرامج ، والمستخدمين والأنظمة امتيازات كافية لأداء مهامهم.
- Should enable to provide privileges when needed and disable them otherwise.
- ينبغي تمكين توفير الامتيازات عند االحاجة وتعطيلها بخلاف ذلك.
- Separate account for each user.
- حساب منفصل لكل مستخدم.

Security and protection Domain of protection مجال الحماية

Domain structure بنية النطاق

- To facilitate this scheme, processes operate within a protection domain.
- لتسهيل هذا المخطط ، تعمل العمليات ضمن مجال حماية.
- Each domain defines a set of objects and the types of operations that may be invoked on each object.
- يعرف كل مجال مجموعة من الكائنات وأنواع العمليات التي قد يتم استدعاؤها على كل كائن.
- Domains are not necessarily disjoint.
- الأشكال ليست بالضرورة منفصلة.

Security and protection Domain of protection مجال الحماية

Domain structure A domain can be realised in a variety of ways:-

بنية المجال يمكن تحقيق النطاق بعدة طرق:-

- Each user may be a domain.
- قد يكون كل مستخدم مجالا.
- Each process may be a domain.
- كل تكون كل عملية مجال.
- Each procedure may be a domain.
- قد يكون كل اجراء مجال.

Security and protection System security نظام الحماية

- Protection is strictly an internal problem.
- تعتبر الحماية مشكلة داخلية بحتة.
- Security, however, requires also consideration of the external environment.
- الأمن، مع ذلك، يتطلب أيضا النظر في البيئة الخارجية.
- A protection system is ineffective, for instance, if user authentication is compromised.
- نظام الحماية غير فعال ،على سبيل المثال ،اذا تم اختراق مصادقة المستخدم.

Security and protection The security problem المشكلة الأمنية

- A threat is a potential for a security violateon.
- التهديد هو احتمال لأنتهاك الأمن.
- An attack is the attempt to break security.
- الهجوم هو محاولة كسر الأمن.

Security and protection The security problem

- Breach of confidentiality .
- خرق السرية .
- Breach of integrity .
- خرق النزاهة.
- Breach of availability .
- خرق التوافر.
- Theft of service .
- سرقة الخدمة.
- Denial of service .
- الحرمان من الخدمة.

Security and protection The security problem

To protect a system, we must take security measures at four levels:
يجب أن تتخذ اجراءات أمنية على أربعةة مستويات:-

- Physical
- Human.
- Operating system.
- Network.

- جسدي-بدني.
- بشري
- نظام التشغيل.
- شبكات الاتصالز

Security and protection Program threats برامج التهديدات

a security thread is most often posed by a program
غالبا ما يشكل تهديدا أمنيا من قبل برنامج

- Trojan horse
- Trap door.
- Logic bomb.
- Stack and buffer overflow.
- Viruses.

- حصان طروادة.
- باب فخ.
- قنبلة المنطق.
- المكدس وتجاوز العازلة.
- الفيروسات.

Security and protection The security problem

Trojan horse : حصان طروادة

- A code segment that misuses its environment is called a Trojan horse.
- يسمى حزء الرمز الذي يسيء استخدام البيئة الخاصة به حصان طروادة.

Security and protection The security problem

Trap door : باب الفخ

- A trap door might also be included in the compiler so that the scan of the source code alone will not reveal the security threat .
- يمكن ايضا ادراج باب اعتراض في المحول البرمجي بحيث لا يكشف مسح الشفرة المصدرية وحده عن التهديد الأمني.
- Trap doors pose a difficult problem since the whole source code has to be scanned in order to detect them.
- تشكل مصائد الأبواب مشكلة صعبة نظرا لأنه يجب فحص شفرة المصدر بأكملها من أجل اكتشافها.

Security and protection The security problem

Logic bomb :القنبلة المنطقية

- A program that initiates a security incident only under certain circumstances is called a Logic bomb It is hard to detect since under normal operations no security hole is apparent.
- يطلق على البرنامج الذي يستهل حادثا أمنيا في ظل ظروف غير مؤكدة أنه من الصعب اكتشافها قنبلة منطقية.لأنه في ظل العمليات العادية لا يظهر ثقب امني.

Security and protection The security problem

Logic bomb :

- A program that initiates a security incident only under certain circumstances is called a Logic bomb.
- القنبلة المنطقية يطلق على برنامج يطلق حادثة أمنية في ظروف معينة فقط قنبلة منطقية.
- It is hard to detect since under normal operations no security hole is apparent.
- من الصعب اكتشافه لانه في ظل العمليات العادية لايوجد ثقب امني واضح.

Security and protection The security problem

Stack and buffer overflow : المكدس وتجاوزالعازلة

- An attacker might write a program to do the following
- قد يقوم المهاجم بكتابة برنامج للقيام بما يلي:

1. Overflow an input field, command line argument or input buffer until it writes into the stack .

- تجاوز حقل الأدخال أو وسيطة سطر الأوامر أو مخزون الأدخال المؤقت حتى يكتب في بنية تخزين العناصر.

2. Overwrite the current return address on the stack with the address of the exploit code to be loaded .

- الكتابة فوق عنوان المرسل الحالي على المكدس مع عنوان رمز الاستخدام المراد تحميله.

3. Place exploit code in the next space of the stack.

- ضع رمز استغلال في المساحة التالية من المكدس.

Security and protection The security problem

Viruses :

- A virus is a fragment of code embedded in a legitimate program .
- الفيروس هو جزء من شفرة مدمجة في برنامج شرعي.
- Viruses are designed to ‘infect‘ other programs .
- تم تصميم الفيروسات "لأصابة" البرامج الأخرى.
- Viruses are typically very specific to architectures, operating systems and applications.
- تكون الفيروسات عادة خاصة جدا بالبينات وأنظمة التشغيل والتطبيقات.