Access Control

Access Control

- Its function is to control which principals (otherwise known as Subjects) have access to which resources (Objects) in the system.

Protected resources: system resources for which protection is desirable
  - Memory, file, directory, hardware resource, software resources, external devices, etc.

Subjects: active entities requesting accesses to resources
  - User, owner, program, etc.

Access mode: type of access
  - Read, write, execute (generally speaking)

Access Control

Access Control Policy for son Ben:

- Allowed access:
  - House
- Disallowed access:
  - Automobile

Access Control

Access Control Policy for son Ben:

- Allowed access:
  - House
- Disallowed access:
  - Automobile

Access Control

Access Control Policy for son Ben:

- Allowed access:
  - House
- Disallowed access:
  - Automobile

Problem!
Unauthorized access

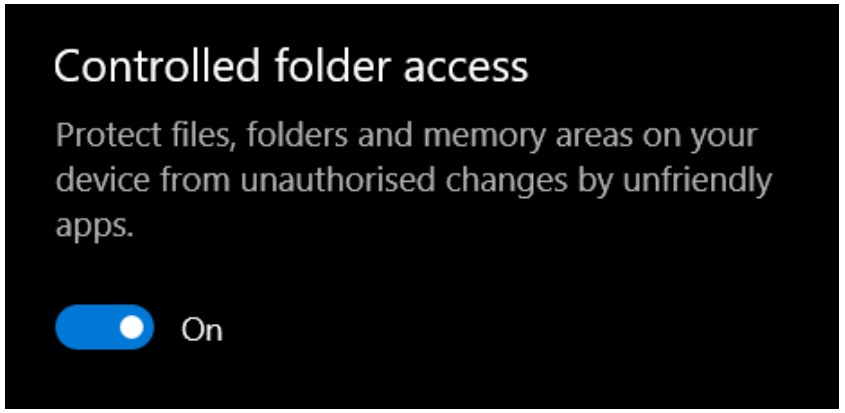
Access Control

Access Control Policy for son Ben:

- Allowed access:
  - House
- Disallowed access:
  - Automobile
  - Car keys

Why do we need Access Control?

- **Access control**: ensures that all accesses to object are authorized
- Protects against accidental and **malicious** threats by regulating the *reading, writing and execution* of data and programs
- Need:
  - Proper ***authorization*** and ***authentication***
    - *Authentication* – who requested access?
    - *Authorization* – who is allowed to access ?



Mechanism

- The access controls provided with an operating system typically:
  - Authenticate principals using a mechanism (passwords or Kerberos)
  - Mediate access to files, communications ports and other system resources.
- Modelled by a matrix of access permissions:
  - columns for files, rows for users.
  - r - read, w – write, x – execute, “-” – no access (might be other access types depending on the object)

Access Control Matrix

Access rights defined individually for each combination of subject and object

- Managing access control:
  - complex in large systems
  - error prone
  - E.g Bank with 50,000 staff and 300 applications = access control matrix has 15,000,000 entries.
    - Performance problem and vulnerable to administrators' mistakes.

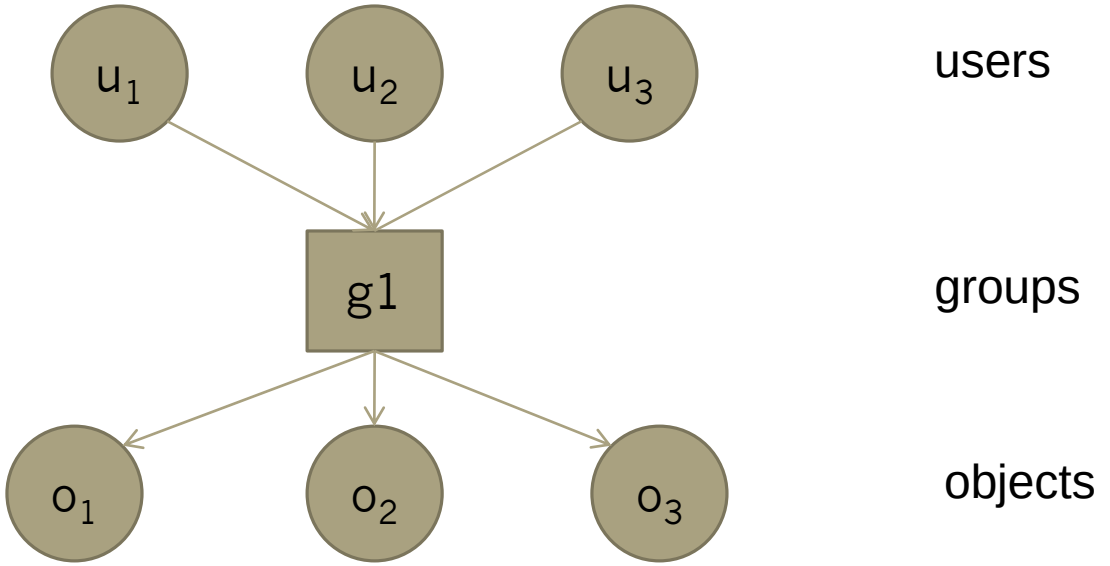
	Marks.doc	**Edit.exe**	**Game.exe**
Alice	-	{execute}	{execute, read}
Bill	{read, write}	{execute}	{execute, read, write}

Solution

- Two main ways:
  - Compress the users:
    - Groups or Roles
  - Compress the rights:
    - ACLs or Capabilities

User Compression - Groups

- Users with similar access rights collected in groups
- Groups are given permissions to access objects



User Compression - Roles

- A role is a collection of permissions
- A user effectively inherits those permissions when he acts under that role.

Rights Compression – Capabilities

- *Capability* – an un-forgeable token specifying the subject's access rights
- Capability lists are usually kept within the address space of the user
- Corresponds to a row in an access control matrix
    - e.g. *Alice's capability: edit.exe: execute, game.exe: execute, read;*
- When a process invokes another process - > capabilities are passed on
- An initial capability list must be generated for a new user (unclear initial list).

	Marks.doc	**Edit.exe**	**Game.exe**
Alice	-	{execute}	{execute, read}
Bill	{read, write}	{execute}	{execute, read, write}

Rights Compression – Access Control List (ACL)

- Access rights to an object stored with the object itself
- Corresponds to the column of access control matrix
    - e.g. *ACL for edit.exe: Alice: execute; Bill: execute;*
- Used in Unix-based systems (Linux and Apple's OS/X)
- Windows access control mechanism is based on ACLs
- Tedious to find all the files to which a user has access

Advanced Protection Techniques

- Sandboxing
- Virtualization
- Trusted Computing

Sandboxing

- Tightly controlled environment where programs can be run
- Technique that isolates programs, preventing malicious or malfunctioning programs from damaging or snooping on the rest of your computer.
- Restricts what a piece of code can do, giving it just as many permissions as it needs (*principle of least privilege).*

What's already being Sandboxed

- **Web Pages**
  - The browser essentially sandboxes the web pages it loads.
  - Restricted to running in the browser and accessing a limited set of resources
  - Web pages can run JavaScript code, if code tries to access a local file on the computer, the request will fail.
- **Browser Plug-in Content**:
  - Content loaded by browser plug-ins (Adobe Flash or Microsoft Silverlight) is run in a sandbox.
- **Windows Programs**:
  - User Account Control functions as a bit of a sandbox, essentially restricting Windows desktop applications from modifying system files without first asking your permission.
  - Very minimal protection.

Sandboxing : Android vs IOS

Android	iOS
App announces permission requirement	Apps have same permissions
Installation-time approval	First-usage time approval
App may have more powerful permissions	Limited permissions

Problem?

- A large numbers of existing applications expect to run as root, so that they can modify registry settings.
- Root can do what it likes — access any file, become any user.
- The root user is typically made available to the system administrator.

.

	Operating System	Accounts Program	Accounting Data	Audit Trail
Sam	rwx	rwx	rw	r
Alice	x	x	rw	–
Bob	rx	r	r	r

Virtualization

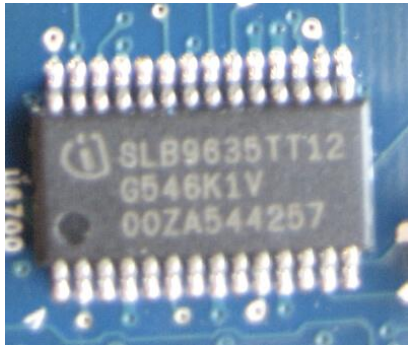
- Virtualization allows people to run a host operating system on top of a guest
- Offers flexibility and the prospect of better containment.
- The Operating system may have the capability to allow or deny access to resources based on which program requests them and the user account in the context of which it runs.
- A program which is expected to perceive the whole computer, once run inside a container, can only see the allocated resources and believes them to be all that is available.
- Vista uses virtualization technology for legacy applications: if they modify the registry, they don’t modify the ‘real’ registry but simply the version of it that they can see.

Trusted Computing : basic idea

- Addition of security hardware functionality to a computer system to compensate for insecure software
- Enables external entities to have increased level of trust that the system will perform as expected/specified
- Trusted Computing = computing on a Trusted Platform
- Trusted hardware example is the Trusted Platform Module (TPM) chip
- https://www.youtube.com/watch?v=XgFbqSYdNK4

TPM

- A smartcard chip mounted on the PC motherboard.
- Monitors the PC at boot time and reports its state to the operating system
- Use TPM to certify to other PCs that it was in an ‘approved’ configuration (remote attestation).



Further Interesting Events

- DEF CON 20 Hacking Conference Presentation By Chris Tarnovsky - Attacking TPM Part 2 A Look at the ST19WP18 TPM Device - Video.mp4
- https://www.bleepingcomputer.com/news/security/researchers-detail-two-new-attacks-on-tpm-chips/