Lecture 15

OS Security

- How are resources protected ?
- How is the access to files controlled ?
- What methods are used for user authentication ?
- What threats do exist ?

Protection

- It is about controlling the access to computer resources; it needs to be specified and then enforced.
- Each process should use only its resources according the stated policies.
- *One principle*: least privilege, meaning that only enough privileges to perform the tasks are granted.
- Domain of protection: a protection domain defines the resources that can be used and for what operations (access rights). *Example*: file xy, read/write.
- Domains can overlap, or processes can switch from one domain to another one (i.e., processes from user to kernel mode).
- Each user/process/procedure can be a domain.

Access matrix

Domain/object	F1	F2	F3	f4
D1	read	read		
D2		read/write	read	execute
D3		read		execute

The content of a cell is a result of the policy . The same applies to process allocation to domains – this is a function of the OS.
Domain switch can be included as a cell corresponding to a domain object. The operation is “switch” from current domain to the column domain.
Another possibility is for a process in a domain to copy the rights regarding an object to other domains.

Access matrix implementation

- *Global table*: set of ordered triples {domain, object, rights}. Generally, this is a large table.
- *Access lists* for objects: one access list for each object of the form {domain, rights}.
- *Capability lists*: a capability list for each domain lists the objects and associated rights.
- *Lock-key*: each object has a list of unique bit patterns (locks) and each domain has a list of unique bit patters (keys). If there is a match, the process in that domain can execute the operation on the object.

Revocation of access rights

- Immediate vs delayed
- Selective vs general
- Partial vs total
- Temporary/permanent

Language-based protection

- Classes running in the same JVM may be from different sources and may not be equally trusted.
- Protection decisions are made within JVM: when a class is loaded, JVM assigns it to a protection domain that gives permissions.
- The protection domain depends on the URL from which the class was loaded and any digital signature on the class file.
- It also uses the stack inspection mechanism as accesses are often performed indirectly, through system libraries or other classes.

User authentication

- The starting point for any security system is to establish who is making the request/ any request.
- As processes have owners/users, any request from a process is considered as coming from its user.
- Before granting the request, the OS checks it against the policy that specifies what that user can do.
- In addition, a user can be member of a group, and therefore has the rights of the group.
- The process of checking a user's identity is called authentication. Techniques for authenticating a user are dependent on the hardware available.
- One method: user names and passwords. Generally, encrypted passwords are stored in a file to whom only the administrator has access.

Cryptographic hashing functions

- Certain hash functions make good one-way encryption functions.
- Hashing functions with 64, 128 or 256 bits of output are quite common.
- One goal is to reduce the probability of collisions.
- The second is to make the discovery of the input as difficult as possible.
- Callbacks are used to minimize the probability of an intruder connecting to a phone line.

Synchronized authentication

- The user and the system use a synchronized random number generator. The generators change periodically, therefore any playback attack fails.
- One issue is that there is a window of opportunity when the scheme works.
- The second is synchronization – the two clocks drift apart over time. The system can adjust itself to the user's generator.
- Another possibility is to have the system sending a message which is encrypted by the user and returned to the system. They use the same encryption key.
- One-time passwords methods such as S/KEY, both start with a shared, secret passphrase. They use hash functions to create passwords. The user will use them in reverse order, n-1, n-2,….3, 2, 1.
- Biometric authentication: fingerprint, iris or retina.