211 – Operating Systems

Tutorial: Security
– Answers –

Lecturer: Peter Pietzuch ⟨prp@doc.ic.ac.uk⟩

1. Why are security and protection important even for computers that do not contain sensitive data?

   Answer: All computers, regardless of the data they manage, are susceptible to security breaches that may crash the system, spread viruses or commit identity theft.

2. Sharing and protection are conflicting goals. Give three significant examples of sharing supported by operating systems. For each, explain what protection mechanisms are necessary to control the sharing.

   Answer: Examples of sharing supported by operating systems are sharing virtual memory regions, sharing processor time between processes and sharing files between users. Virtual memory regions can be shared by multiple processes; operating systems provide protection via page and segment table entries, and processors enforce memory protection by checking these entries against memory references. A system's processor is multiplexed among the system's processes; to prevent a process from monopolizing a processor, operating systems set timer interrupts. File systems enable multiple users to share data stored in files; operating systems provide access control lists (or similar access control mechanisms) and encryption to prevent unauthorized users from accessing file data.

3. Explain what one-way functions are and give an example of how they are used in practice.

   Answer: A one-way function is a function f where it is easy to compute f(x) = y but hard to compute x given y. In most operating systems, passwords are encrypted using a one-way function in order to prevent attackers, including system administrators trying to abuse their privileges, from obtaining the passwords.

4. Why are passwords in UNIX stored together with a salt value?

   Answer: The salt value ensures that the same password will result in a different encrypted version. It also means that encrypted passwords are specific to the chosen salt value, so a single dictionary for a dictionary attack cannot be pre-computed and reused to attack multiple accounts.

5. What is the principle of least privilege and why does it make sense?

   Answer: The principle of least privilege states that each user, program, process, or entity in general be granted the minimal amount of privilege it needs to accomplish its designated tasks. It makes good sense as a system structuring principle because without excess privilege, entities can not accidentally or maliciously perform actions or modify data they are not supposed to.

6. Represent the ownerships and permissions shown in this UNIX directory listing as an access control matrix. Treat each of the two users and two groups as principals.

   Note: `a` is a member of `users` and `systems`, `b` is a member of `users` only.

```
-rw-r--r--  3 a   systems    4137 2010-03-16 14:19 .emacs
-rwxr-xr-x  3 b   users      6420 2010-03-16 14:19 os.pptx
-rw-rw----  1 b   systems    1997 2010-03-16 14:19 notes.txt
-rw-r-----  3 a   users      7442 2010-03-16 14:19 index.html
```

   Answer:

	.emacs	os.pptx	notes.txt	index.html
a	r,w	r,x	r,w	r,w
b	r	r,w,x	r, w	r
users	r	r,x	-	r
systems	r	r,x	r,w	-