10.1 Operating System Security Reading

Notebook:	How Computers Work [CM1030]		
Created:	2019-10-09 10:09 AM	**Updated:**	2019-11-28 4:11 PM
Author:	SUKHJIT MANN		

Cornell Notes	**Topic:** 10.1 Operating System Security-Reading	Course: BSc Computer Science Class: How Computer Work [CM1030]-Reading Date: November 28, 2019

Essential Question:

What are security measures are in place on an Operating System to make sure the environment and the user are safe?

Questions/Cues:

- What is an account?
- What is a login procedure?
- What is an administrator/Super-user?
- What is auditing software?
- What is privilege/ non-privileged mode?

Notes

- Account = a record within OS containing entries such as user's name, password and privileges to be granted to that user.
- Login procedure = a sequence of transactions in which user establishes initial contact with a comp's OS
- Administrator/Super-user = establishes accounts on OS, gains high privileged access to OS by identifying as admin during login. From here, admin can alter settings within OS, modify critical software packages, adjust privileges granted to other users & perform variety of other maintence activities that denied to normal users
  - Also being a super-user, an admin is able to monitor activity with comp system in an effort to detect destructive behavior, whether malicious or accidental
- Auditing software = record and then analyze the activities taking place within comp system.
  - may also identify activities within user's account that don't conform to that user's past behavior
  - Also designed to detect the presence of sniffing software, software when left running on comp records activities and later reports them to a would-be intruder.
- CPU's designed for multi-programming systems contain special-purpose registers in which OS can store upper & lower limits of a process's allotted memory area. If process outside allotted area, CPU does interrupt sequence to transfer control back to OS. Even so, process could merely change upper-limit of SP-register for more memory without permission of OA

    - To counteract this, multi-programming CPU's designed to operate in two privilege levels, "privilege mode" & non-privileged mode"
- Privileged mode = CPU able to execute all instructions in its machine lang. Also it can execute special instructions only available in privilege mode called privileged instructions
    - list of acceptable instructions in non-privileged mode is limited
    - Examples of privileged instructions are: instructions that change contents of memory limit registers & instructions that change current privilege mode of CPU
    - Attempt to execute privilege instruction when CPU in non-privileged mode causes an interrupt. Interrupt converts CPU to privilege mode & transfers control to interrupt handler within OS
- When comp first turned on, CPU is in privileged mode, when OS starts at end of boot process, all instructions are executable

Summary

In this week, we learned about the types of different users on an OS and building on this further, we explored how a similar relationship exists in the levels of machine instruction.