CIS 452 - Operating Systems Concepts

Nathan Bowman

Images taken from Silberschatz book

Security

Protection measures, such as access control lists, are important starting point

However, ACLs will not help if unauthorized user somehow gains root access to system

Textbook distinguishes between *protection*, such as ACLs, and **security** -- ensuring system resources used and accessed only as intended

Security must take into account external environment, such as malicious actors guessing user's password or user downloading harmful software

Security is large subject, and we won't even scratch the surface

Need to ensure that both data *and* code on system remain private, cannot be modified without approved access, and are available when users need them

Must consider not just OS, but also physical, network, and *human* aspects

No amount of OS security will help if you respond to that phishing email with your password (though OS can work to mitigate damage by constraining access to only what is needed)

Just some fun terms you might come across (read your textbook for details, or, better yet, take a security course)

Trojan horse -- harmful software "disguised" as something else. For example, text editor that scans files for confidential information and emails it elsewhere

Trap door -- security vulnerability that can be used only in special circumstances, such as a program that ignores usual security checks only when started by user with particular user ID

Logic bomb -- program that initiates security incident only under certain circumstances. For example, if malicious user is fired, logic bomb activates and erases all files on company server

Stack/buffer overflow -- take advantage of lax array-bounds checking to overwrite return address of function to point to malicious code that then runs with escalated privileges

Virus -- fragment of malicious code that replicates itself and is attached to other, non-harmful code. Come in many varieties and do lots of nasty things

Encryption is an important topic that we do not have time to do justice

Essence of encryption is changing representation of information so it can be read only by authorized parties

Gist: "scrambling" information so it appears random but can be "descrambled" by someone with correct password, key, etc.

Encryption can be used to protect confidentiality of information stored on disk

Access control policies apply only while OS is active

If computer booted with different OS, unencrypted disk can be mounted and read regardless of permissions (it's all just bytes)

```
$ lsblk
NAME                 MAJ:MIN RM   SIZE RO TYPE  MOUNTPOINT
nvme0n1              259:0    0 953.9G  0 disk
├─nvme0n1p1          259:1    0   300M  0 part  /boot
├─nvme0n1p2          259:2    0   128M  0 part
├─nvme0n1p3          259:3    0 250.7G  0 part
├─nvme0n1p4          259:4    0   523M  0 part  /mnt
└─nvme0n1p5          259:5    0 702.3G  0 part
  └─cryptlvm         254:0    0 702.3G  0 crypt
    ├─rootvol-swap   254:1    0     6G  0 lvm   [SWAP]
    ├─rootvol-var    254:2    0    32G  0 lvm   /var
    ├─rootvol-root   254:3    0    32G  0 lvm   /
    └─rootvol-home   254:4    0 632.3G  0 lvm   /home
nvme1n1              259:6    0  27.3G  0 disk
```

```
# mount /dev/nvme0n1p3 /mnt
```

```
# ls /mnt
'$Recycle.Bin'               install.res.1028.dll   ProgramData
'Documents and Settings'     install.res.1031.dll  'Program Files'
 eula.1028.txt               install.res.1033.dll  'Program Files (
 eula.1031.txt               install.res.1036.dll   Recovery
 eula.1033.txt               install.res.1040.dll   swapfile.sys
 eula.1036.txt               install.res.1041.dll   System
 eula.1040.txt               install.res.1042.dll   System64
 eula.1041.txt               install.res.2052.dll  'System Volume I
 eula.1042.txt               install.res.3082.dll  'User Manual'
 eula.2052.txt               Intel                  Users
 eula.3082.txt               Mono                   VC_RED.cab
 globdata.ini                mono.msi               vcredist.bmp
 install.exe                 pagefile.sys           VC_RED.MSI
 install.ini                 PerfLogs               Windows
```

If drive is unencrypted, anyone with access to computer can read it without specialized tools

Encryption can be done on file-by-file (or directory-by-directory) basis, encrypting only information deemed to be important

Or, with full-disk encryption, entire file system encrypted

With full-disk encryption, entire disk *not* unencrypted when computer boots

Instead, information decrypted/encrypted when moved into/out of memory

Data on disk always remains encrypted

With correct OS/driver support, process can often be transparent to applications

Will take some performance hit -- may or may not be noticeable with modern hardware

Encryption not just for privacy of data -- can also help prevent tampering with executables

On unencrypted drive, possible to swap out `ls` for `ls-and-post-all-your-information-online` executable

Encrypted drive can be overwritten with nonsense, but not possible to make malicious changes to executables