Security

Modern Operating Systems, by Andrew Tanenbaum

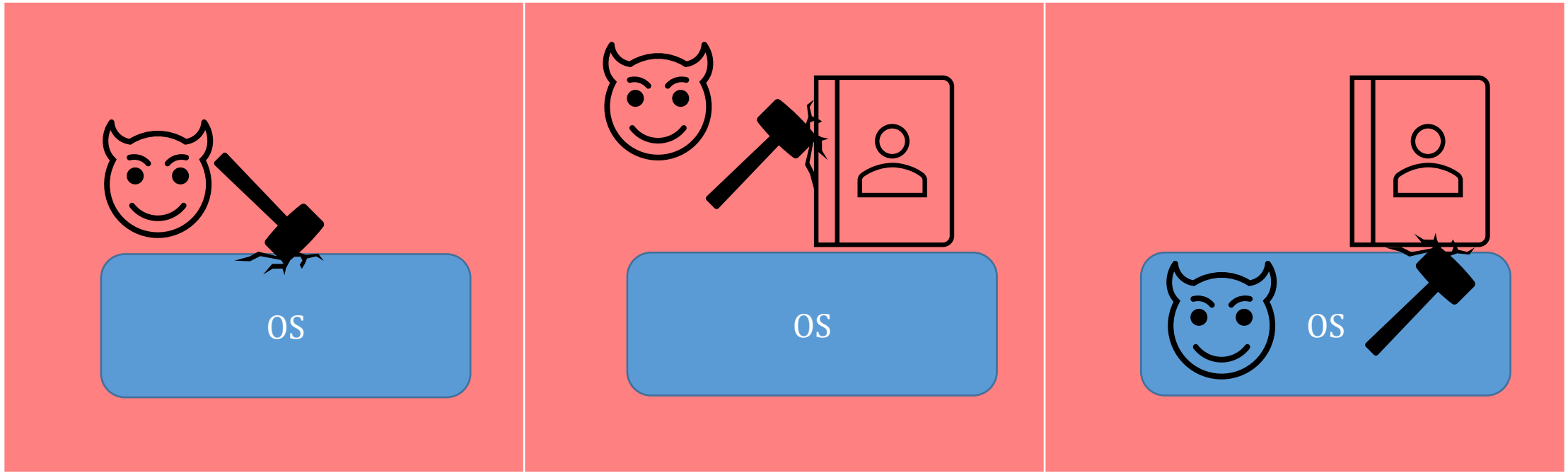
Chap 9

From: https://syslog.com/~jwilson/pics-i-like/kurios119.jpg

What is Security – C.I.A

	Goal	Threat	Prevent bad people from:
C	Data Confidentiality	Exposure of Data	Stealing your data
I	Data Integrity	Alteration of Data	Tampering with your data
A	System Availability	Denial of Service	Doing your work

Securing what from whom?



OS from User	One user from Another	User from OS
OS mechanisms (syscall…)	Access control, Isolation	?

First Level of Defense - Logon

- Logons provided only to "good" users
- If we accidentally give a logon to a bad user, at least we can trace who did what

User Authentication

- Verifying that you are who you claim you are

- Basic Principles: Authenticate using
  - Something the user knows (e.g. password)
  - Something the user has (e.g. ID card)
  - Something the user is (e.g. fingerprint)

- Authenticate BEFORE giving access to
  - Resources, data, files, etc.

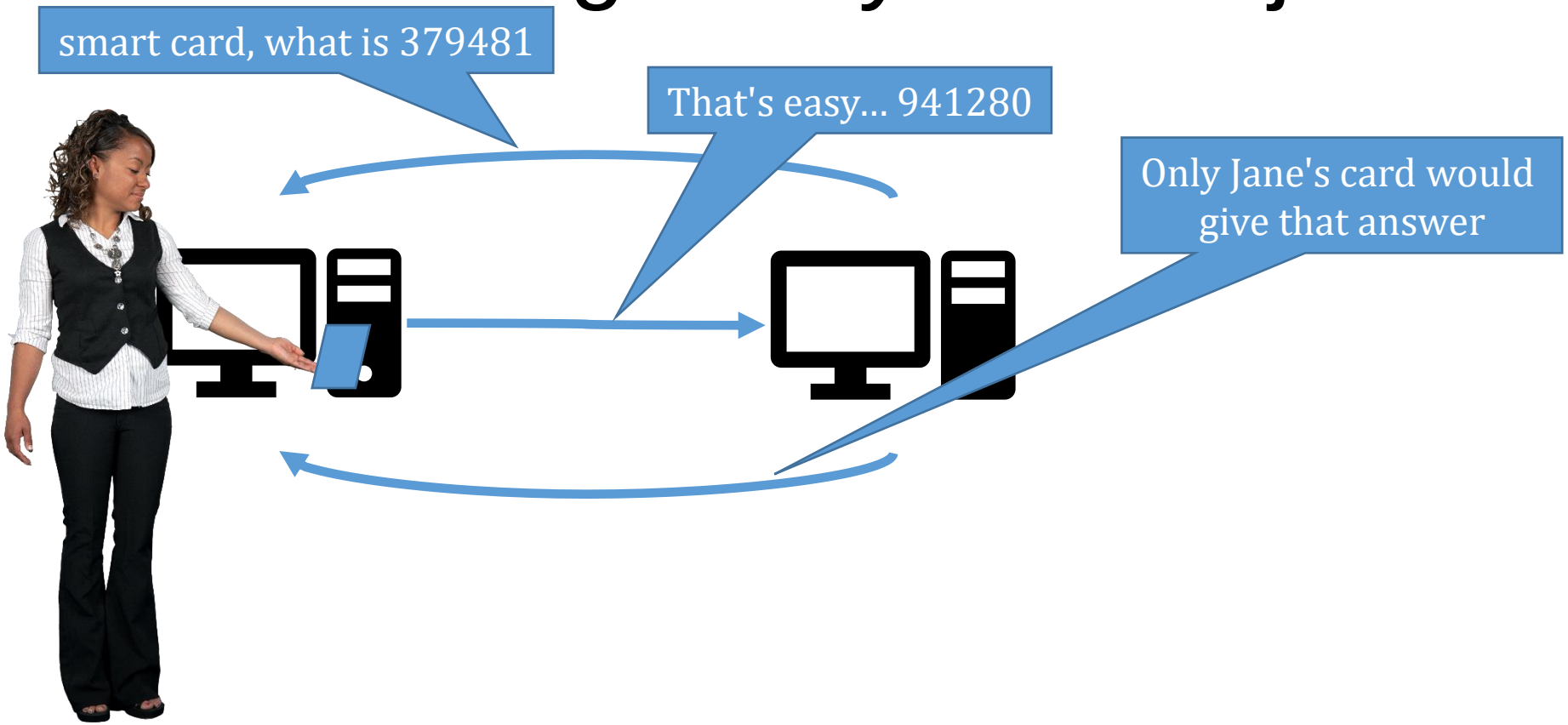
Authentication via Password

- Require user to enter a valid userid and password
- Originally, password stored as plain text in a "protected" file
  - Problem – Requires trusted system administrator
  - Problem – if password file is lost, how to recover?
- Better Alternative: One-way encryption/hash
  - Encryption function enables simple $y=f(x)$, but difficult $x=f^{-1}(y)$
  - When password created, store $y=f(pw)$
  - When password entered, compare $y'=f(pw')$ to y
- But it's easy to FORGET a password!

Challenge/Response Authentication

- Ask user something that no one else would know.
  - Poor choices: Mother's maiden name, where you were born, first girlfriend/boyfriend, pet's name, high school, childhood street, etc.
  - Most information is available on-line, and/or easily guessed
- Ask user something that a computer might find hard to answer
  - "What is the fifth smallest prime number?", but IBM Watson beat Jeopardy champions.
  - "Which of these pictures contain a lamp-post?", but machine learning is making these kinds of questions obsolete.

Authentication using a Physical Object



Works until the smart card is lost or stolen.

Authentication using Biometrics

- Voice, face, fingerprint, iris scan, typing style, signature

- Subject to false-positives
  - Joe's twin got into Joe's account! Their face looks the same.
- Subject to false negatives
  - I broke up with my girlfriend, and have been crying so much the computer can't recognize my iris!
- Susceptible to spoofing attacks
  - Spy movies with a plastic "fingerprint"

Authentication Counter-Measures

- Limit login times – "Sorry, no logins after midnight."
- Limit number of login tries – "Too many invalid attempts… locked"
- Two-factor authentication
  - Password + callback/SMS to specified number
- Logging – "Your last login was Tuesday from Tanganyika"
- Ask user to recognize text in a figure
  - Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA)
- Honeypot Accounts: Simple login name/pw
  - Security notified of all logins
  - Only useful if you are willing to track and catch intruders

Common Motivation of Attackers

1. Peeping Tom – Casual prying by nontechnical users
2. Insider threat – Disgruntled developers, back door
3. Extortion – Personal gain (money, reputation, etc.)
4. Espionage – Commercial, military, or government intelligence
5. Hacktivism – Political or Social motivation

6. Combinations of the above

Common Attacks

and some countermeasures

Trojan Horses

- Convince authenticated user to run your malware
- Malicious email attachments
  - Don't open, open in a VM, use cloud based email reader
- Malicious website that exploits browser vulnerabilities – visit and get hacked
  - Turn off Flash plugins and Javascript – affects usability
- "Free" software actually contains malware
  - Run in VM, don't download
- Place altered version of utility software in libraries
  - Administrator must strictly control file permissions

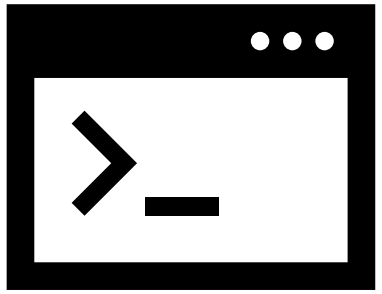
Virus and Worm

- Virus – a program that can reproduce itself by attaching its code to another program
  - Typically contained within a single machine
  - May be spread to other machines via other mechanisms (e.g. human, etc.)

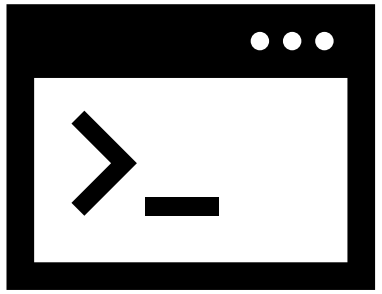
- Worm – a program that automatically reproduces itself, possibly using the network
  - Just reproduction can bring a network to its knees
  - e.g. Stuxnet

Login Spoofing

Correct Login Screen:



Phony Login Screen:



I'm sure I entered the right password.
What happened?

Countermeasures:

- Intentionally enter a fake password the first (few) time(s)
- Use a "trusted path" – e.g. start with Ctrl-Alt-Del to make sure OS puts up login screen

Phishing

- Countermeasures
  - Never share personal information
  - Double check sender, etc.
  - Use the "stink test"

From: IT@Bingamton.ned
Dear Joe,

The Bingamton University IT department has encountered a major problems with machines and require you to reply sending your Bingamton userid and password so that we can fix errors. Please reply now or your userid must be revoked and all files deleted.

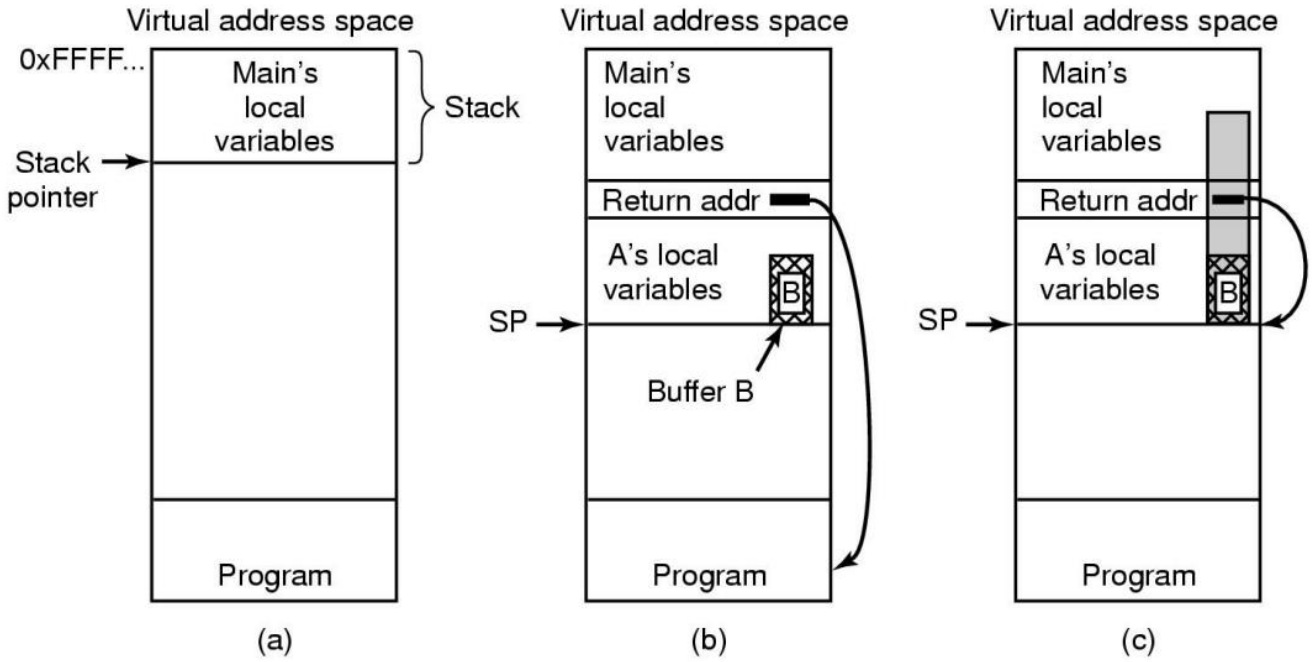
John Jones, IT

Logic Bombs

- Employee writes malware and installs it on the company system
- Malware is not triggered as long as employee logs on five times a week.
- If employee is fired, bomb "explodes"

- Countermeasures: Log activity – easy to correlate and detect.
  - Don't try this at work – your employer may be smarter than you think!

Buffer Overflow



- Buffer length specification in "read" syscall
- Memory protection – don't allow writable memory (stack) to be executed
- Address Space Layout Randomization (ASLR)
- Stack Guards

Dumpster Diving

- Request memory, disk space, tapes
- Read uninitialized data
  - Assume old data is not erased
  - May find passwords, ssh keys, emails, personal info, browsing history, etc.

- Scrub memory/storage after using
- Encrypt data – when finished, erase key
  - (Both take extra effort and time)

Other Methods

- Try executing system calls to see what happens
- Do things you are explicitly told NOT to do
  - ¾ of IBM's security was not describing the security holes
- Convince a system programmer to add a back door
- Make password regulations so strict that user's HAVE to write down passwords and put them on sticky notes on their terminal

Security Design

Logging

- A record of system activity, annotated with time
- Events always added – never erased
- Logs must be analyzed to identify suspect activity
- What to log?
  - Too much logging takes up storage, slows down normal operations, and slows down analysis
  - Too little logging and you miss critical events
- Privacy risk – be aware of privacy laws

Design Principles

- Default should be no access
- Check for current authority
- Give each process the least privilege possible
- Protection mechanisms should be simple, uniform, and in the lowest layers of the system
- Scheme should be simple and psychologically acceptable
  - If it is too hard, user's will get around it

Sandboxes

- Run downloaded code and browser in VM or Container ("Jail")
- Isolate trojans, viruses, worms
- Effectiveness of isolation is only as effective as the security of the sandbox
- VM Escapes and Jail-breaks are possible
  - Usually due to bugs in the implementation of the hypervisor or runtime

OS Security Levels

- Unix has always had "Kernel" level and "User" level
  - Kernel has more privileges
  - Kernel allowed to use privileged instructions and access more memory
- Privilege level is part of the CPU state, managed in HW register
- System call : gateway that enables security level transition
  - On entry, switch to privilege state
  - On return, switch back to user state
- System call is the ONLY way to change security state
- Multiple security levels can be supported (x86 has four…0,1,2,3)

File Permissions

- UNIX tracks Userid of authenticated users and "Group" ID
  - Group ID specified by administrator when userid is created
- Directories/Files have three sets of permissions:
  - Owner, Group, Other
    - If you have same userid as the owner, you get owner permissions
    - Else if you are in the same group as the owner's group, you get group permissions
    - Else you get "other" permissions
  - Each set has R, W, X bits
  - Must have W to directory to create a file in that directory
  - Specify permissions when file is created, or change with "chmod"
  - Change owner with "chown"

Memory Protection

- The execve system call loads an executable from disk
  - User must have permission to execute that file!
  - Executable contains "segments" (code segment, data segment, etc.)
  - Memory protection bits described per segment (R, W, X)
    - Code is "RX", Read only memory is R, Globals are RW, etc.
  - Execve maps these protection bits to pages table entries
- OS knows every memory access and it's purpose
  - Read / Write / instruction-fetch (X)
  - Checks to see if the purpose matches page table entry permissions
  - If not, issues a segmentation violation
- Note: Program can modify permissions for pages – but why?

Access Control

- What permissions are granted to which users
- DAC - Discretionary Access Control (Commodity systems)
  - John can access X, Alice can do Y
- RBAC - Role Based Access Control (Enterprise systems)
  - CEO can do X, Software Engineer can do Y, Secretary can do Z
  - Administrative Role Based Access Control : Dean call allow Department Chair to do X, Dept. chair can allow secretary to do Y
- MAC – Mandatory Access Control (Military, Spy)
  - Multi-level security…

Multi-Level Security

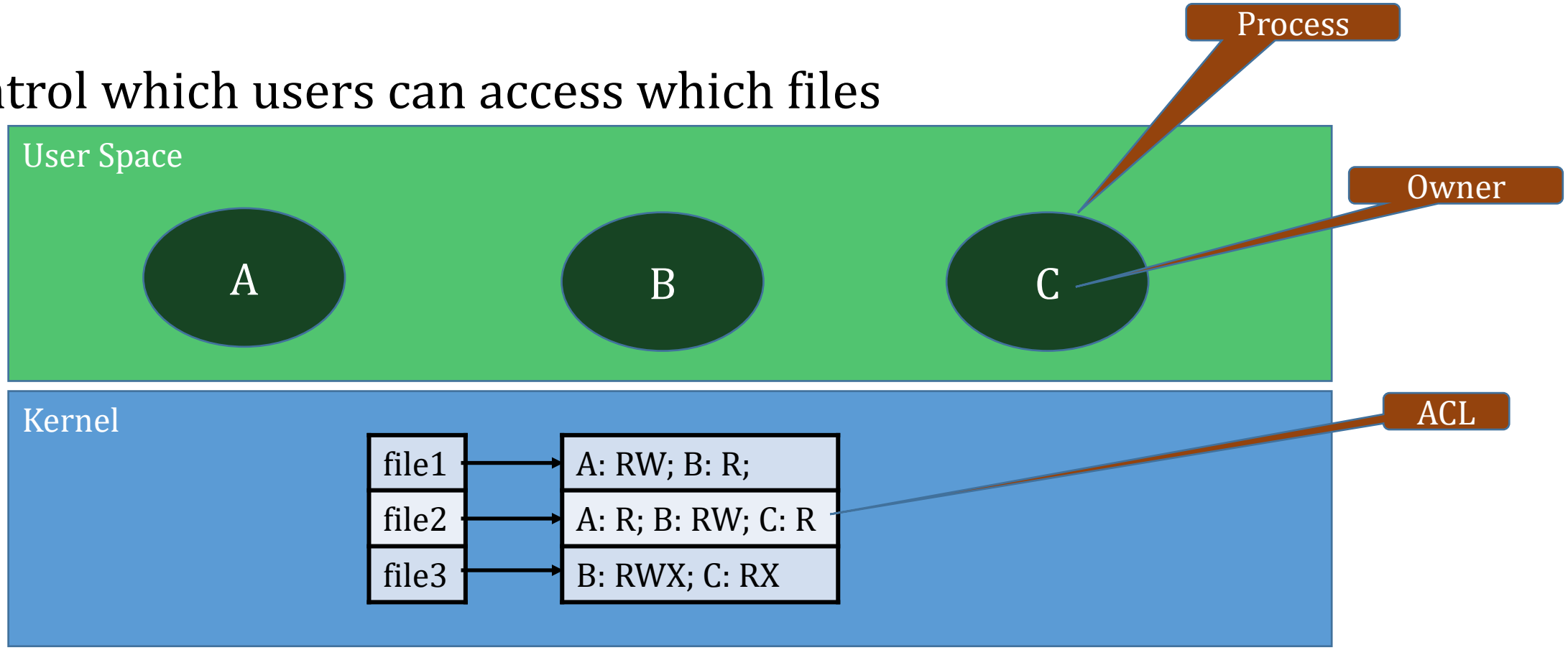
- Data Objects are classified at different levels
  - Top Secret, Secret, Confidential, Unclassified, etc.
  - Sometimes additional compartments: Crypto, Subs, NoForn
- People and Computers have clearances
  - To see a data object, you must have clearance for that level / compartment
- Policy: No read up, No write down
  - People with lower level classifications cannot read higher level documents
  - People with higher level classifications should not write documents with lower level classifications
  - Read down and write up are allowed

Multi Level Security Pump

- Upper-level must acknowledge receipt of data from lower-levels
  - Acknowledgement gives lower level back-door access to information
- An MLS Pump restricts the bandwidth for acknowledgements
  - Allows acknowledgements from higher to lower levels, but
  - Keeps the rate at which acknowledgements are sent so low that interception becomes impractical

Access Control List (ACL)

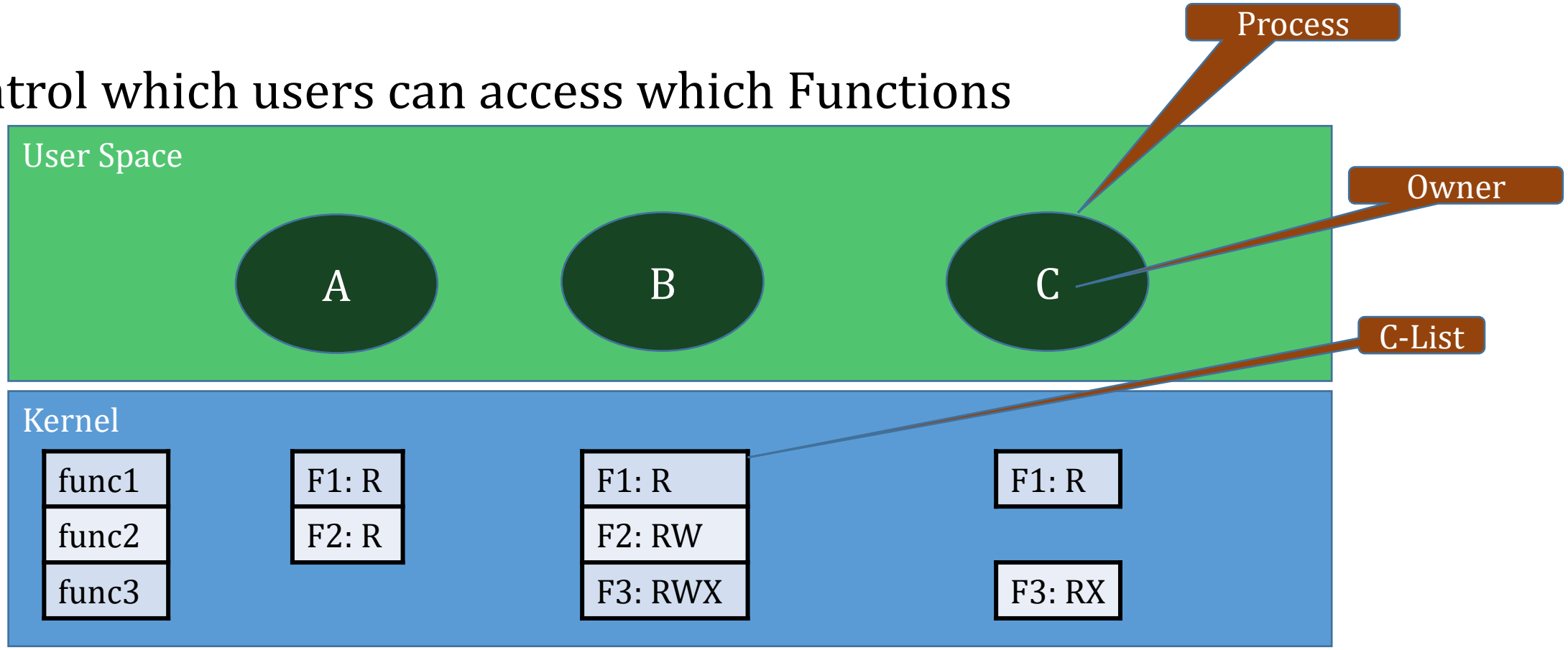
- Control which users can access which files



- Extension of Owner / Group / Other default

Capabilities (C-List)

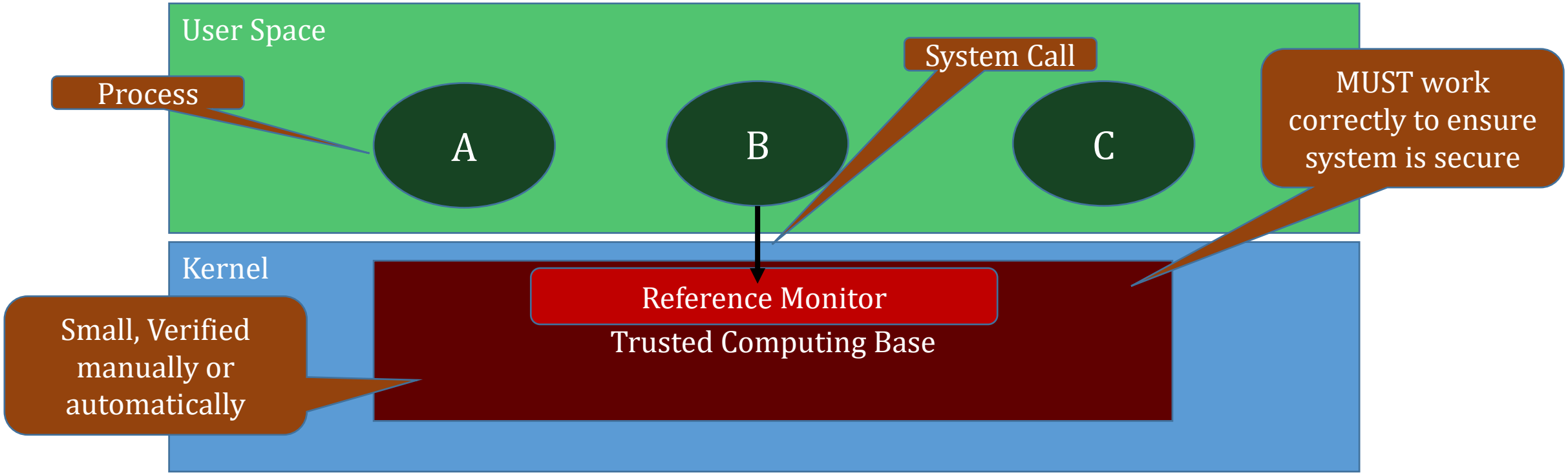
- Control which users can access which Functions



- Like file permissions, but apply to functions

Reference Monitor / Trusted Base

- Enforces access control / capabilities – a.k.a. security kernel



- System calls go through Reference Monitor for Security Checking