CYENG 312/GECE 594 :

Trusted Operating System (OS)

Lecture 07:

1. Auditing and Hardening

2. Access Control

Instructor: Shayan (Sean) Taheri, Ph.D.

Assistant Professor

The Department of Electrical and Cyber Engineering (ECE)

The Institute for Health and Cyber Knowledge (I-HACK)

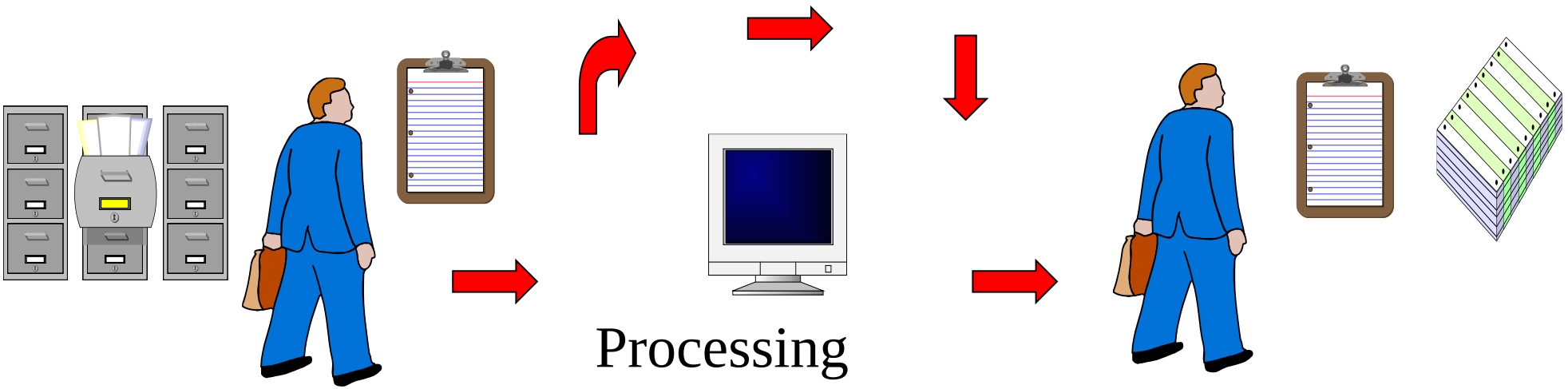
The Gannon University (GU)

Personal Information

- Name: Shayan (Sean) Taheri.
- Date of Birth: July/28/1991.
- Past Position: Postdoctoral Fellow at University of Florida.
- Ph.D. Degree: Electrical Engineering from the University of Central Florida.
- M.S. Degree: Computer Engineering from the Utah State University.
- University Profile: https://www.gannon.edu/FacultyProfiles.aspx?profile=taheri001

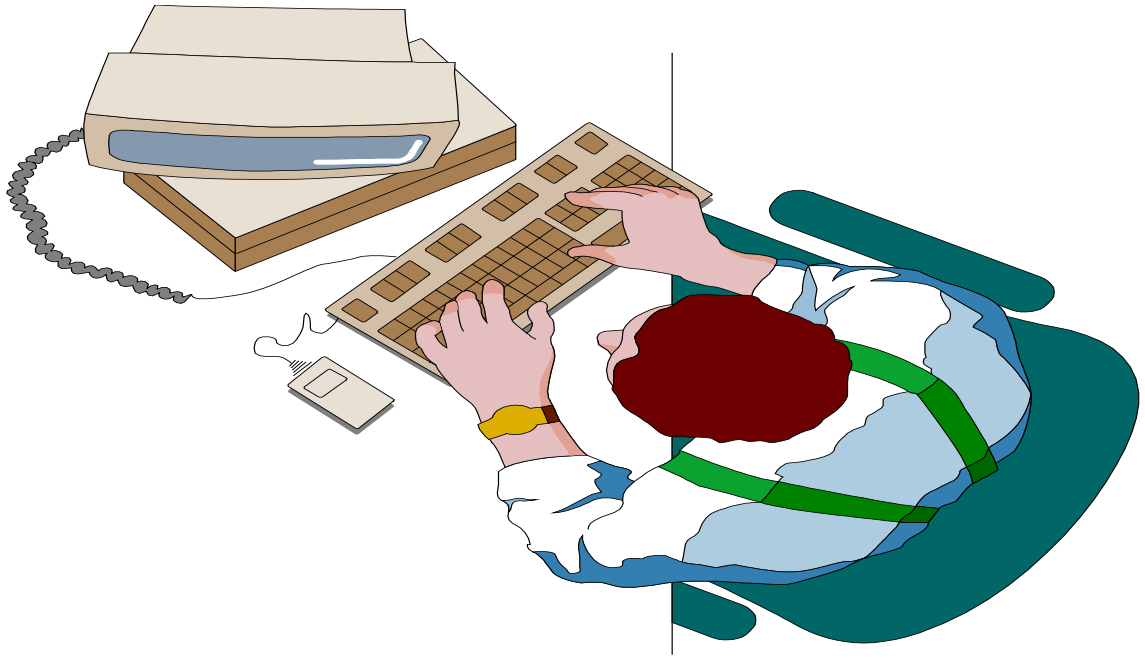
Auditing Around the Computer

- The auditor ignores computer processing.
- Instead, the auditor selects source documents that have been input into the system and summarizes them manually to see if they match the output of computer processing.



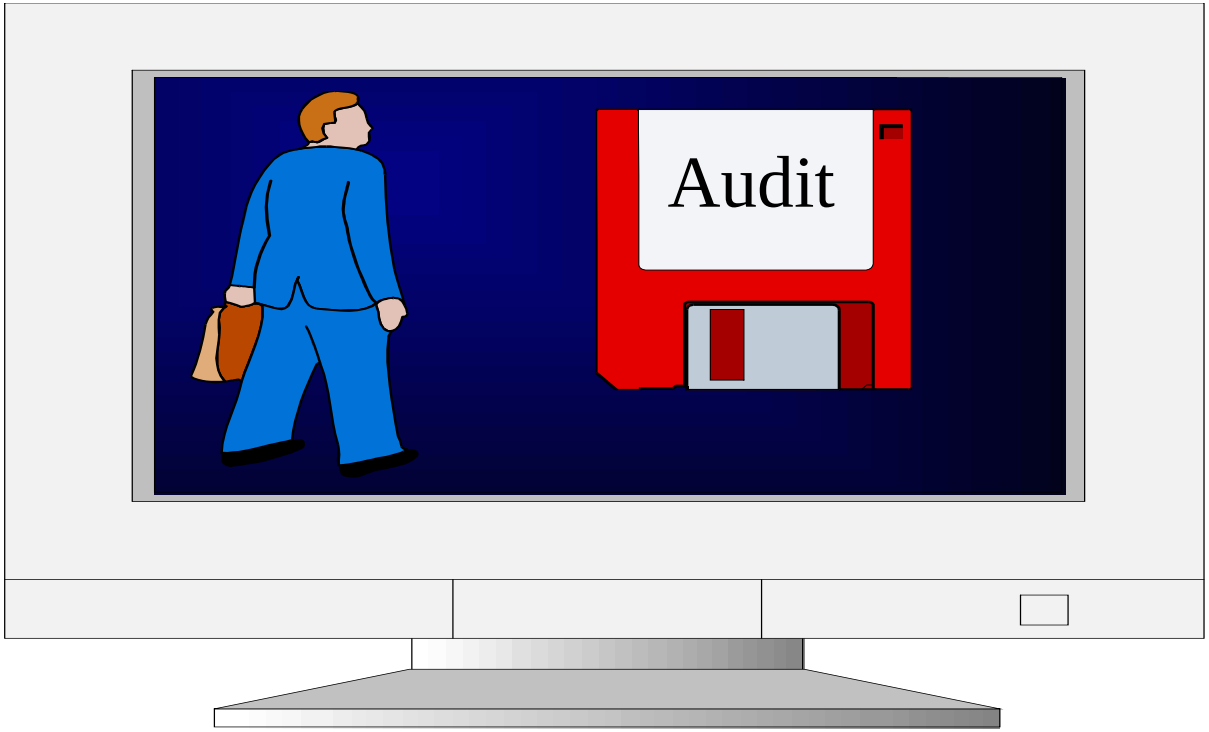
Auditing With the Computer

- The utilization of the computer by an auditor to perform some audit work that would otherwise have to be done manually.



Auditing Through the Computer

- The process of reviewing and evaluating the internal controls in an electronic data processing system.



Audit Software

- Computer programs that permit computers to be used as auditing tools include:
  - Generalized audit software:
    - ✓ Perform tasks such as selecting sample data from file, checking computations, and searching files for unusual items.
  - PC Software:
    - ✓ Allows auditors to analyze data from notebook computers in the field.

Embedded Audit Routines

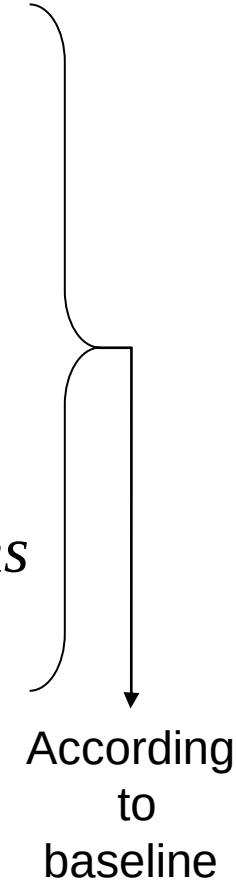
- In-line Code – Application program performs audit data collection while it processes data for normal production purposes.
- System Control Audit Review File (SCARF):
  - Edit tests for audit transaction analysis are included in program.
  - Exceptions are written to a file for audit review.

Application Hardening

- Make your computer hard to break.
- Providing protection to your computer system.
- Protection is provided in various layers like at the host level, the application level, the operating system level, the user level, the physical level and all the sublevels in between.
- Each level requires a unique method of security.

Elements of Hardening

- Physical security
- Secure installation and configuration
- Fix known vulnerabilities
- Remove/Turn off unnecessary services (applications)
- Harden all remaining applications
- Manage users and groups
- Manage access permissions
  - *For individual files and directories, assign access permissions to specific users and groups*
- Back up the server regularly
- Advanced protections



Hardening Activities for Computer

- Keeping security patches and hot fixes updated
- Monitoring security bulletins that are applicable to a system's operating system and applications
- Installing a firewall
- Closing certain ports such as server ports
- Not allowing file sharing among programs
- Installing virus and spyware protection, including an anti-adware tool so that malicious software cannot gain access to the computer on which it is installed
- Keeping a backup, such as a hard drive, of the computer system

Hardening activities for Computer (Cont.)

- Disabling cookies
- Creating strong passwords
- Never opening emails or attachments from unknown senders
- Removing unnecessary programs and user accounts from the computer
- Using encryption where possible
- Hardening security policies, such as local policies relating to how often a password should be changed and how long and in what format a password must be in

Windows Hardening

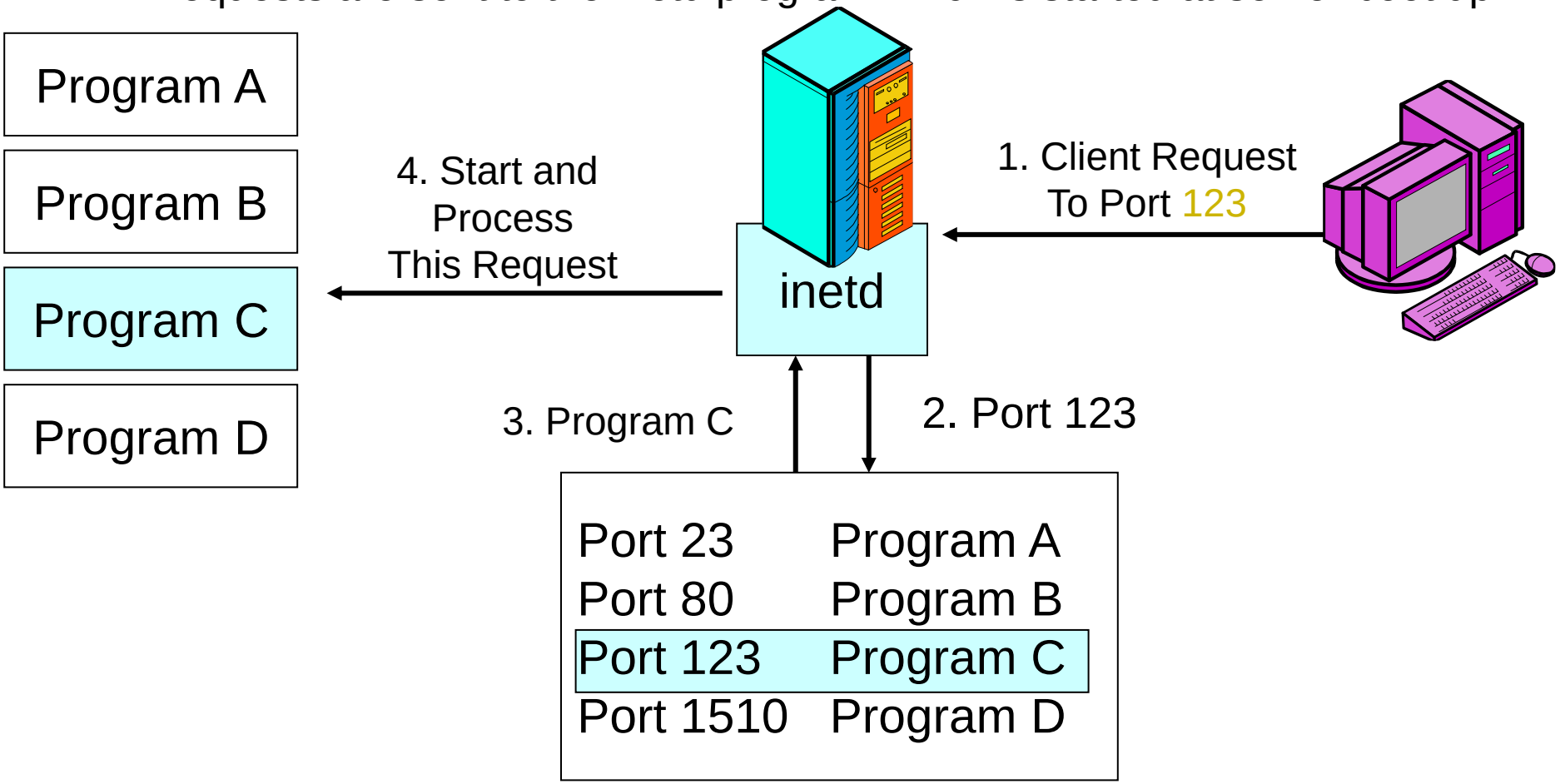
- Use NTFS on all the partitions
- Disabling simple file sharing
- Disable guest account
- Installing antivirus software on computer
- Encrypt temp folder
- Install latest service packs
- Implementing IPSec

Linux Hardening

- Create firewall
- Use secure alternatives
- Copy your logs
- Enable password aging
- Keep an eye on open files

Linux Hardening (Cont.)

- Starting services upon client requests
  - Services not frequently used are dormant
  - Requests do not go directly to the service
  - Requests are sent to the inetd program which is started at server boot up



Access Control

- The process by which resources or services are granted or denied on a computer system or network
- There are four standard access control models as well as specific practices used to enforce access control

Access Control Terminology

- **Identification**
  - *A user accessing a computer system would present credentials or identification, such as a username*
- **Authentication**
  - *Checking the user's credentials to be sure that they are authentic and not fabricated, usually using a password*
- **Authorization**
  - *Granting permission to take the action*
- A computer user is granted **access**
  - *To only certain services or applications in order to perform their duties*

➢ **Custodian**

❑ *The person who reviews security settings*

- *Also called **Administrator***

Access Control Terminology (Cont.)

Action	Description	Scenario Example	Computer Process
Identification	Review of credentials	Delivery person shows employee badge	User enters username
Authentication	Validate credentials as genuine	Megan reads badge to determine it is real	User provides password
Authorization	Permission granted for admittance	Megan opens door to allow delivery person in	User authorized to log in
Access	Right given to access specific resources	Delivery person can only retrieve box by door	User allowed to access only specific data

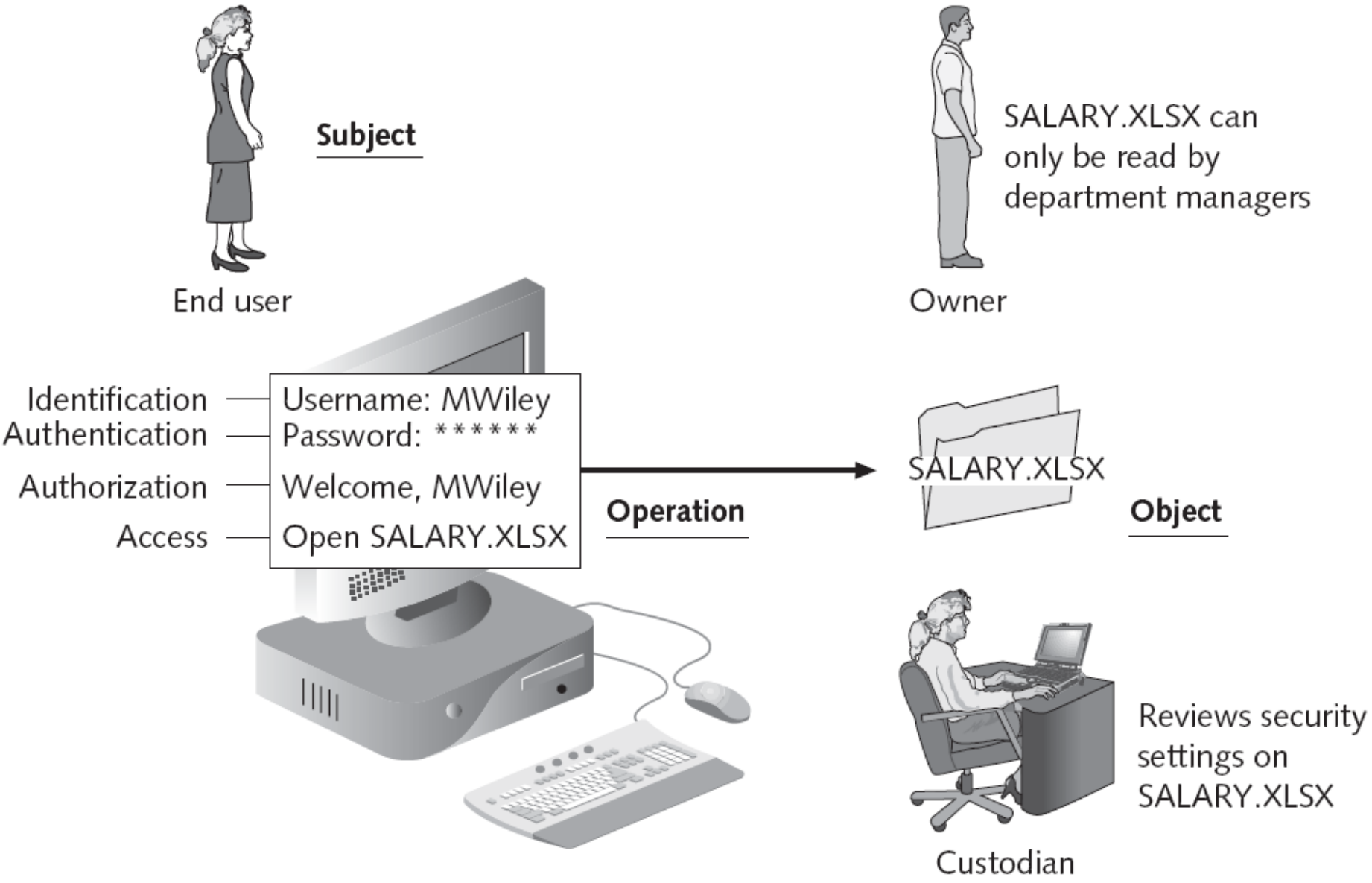
Access Control Terminology (Cont.)

- Computer access control can be accomplished by one of three entities: hardware, software, or a policy
- Access control can take different forms depending on the resources that are being protected
- Other terminology is used to describe how computer systems impose access control:
  - ***Object*** *– resource to be protected*
  - ***Subject*** *– user trying to access the object*
  - ***Operation*** *– action being attempted*

Access Control Terminology (Cont.)

Role	Description	Duties	Example
Owner	Person responsible for the information	Determines the level of security needed for the data and delegates security duties as required	Determines that file SALARY.XLSX can be read only by department managers
Custodian	Individual to whom day-to-day actions have been assigned by the owner	Periodically reviews security settings and maintains records of access by end users	Sets and reviews security settings on SALARY.XLSX
End User	User who accesses information in the course of routine job responsibilities	Follows organization's security guidelines and does not attempt to circumvent security	Opens SALARY.XLSX

Access Control Terminology (Cont.)



Access Control Models

- Mandatory Access Control
- Discretionary Access Control
- Role-Based Access Control
- Rule-Based Access Control

Mandatory Access Control (MAC) Model

- Most restrictive model—used by the military
- Objects and subjects are assigned access levels
- Unclassified, Classified, Secret, Top Secret
- The end user cannot implement, modify, or transfer any controls

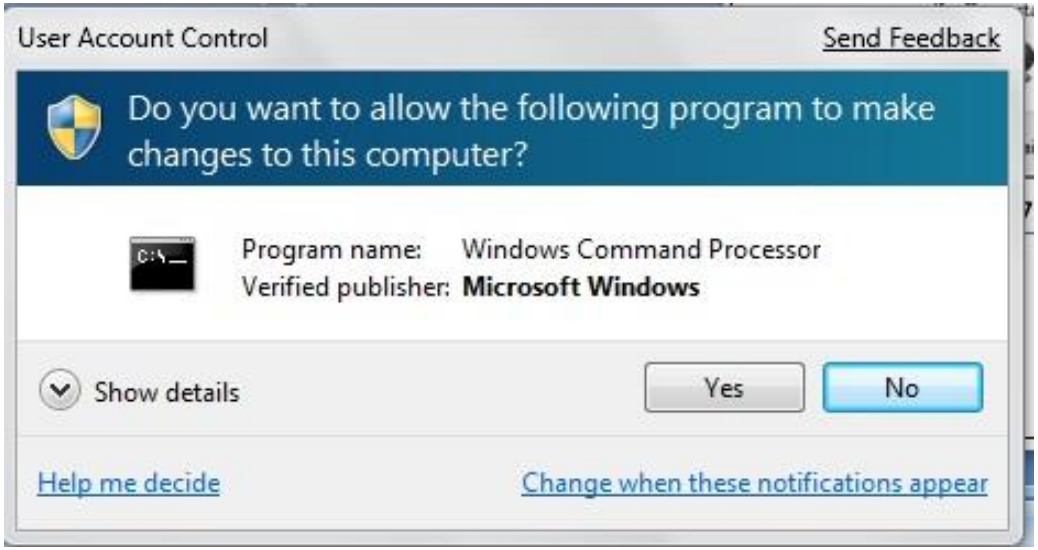
Discretionary Access Control (DAC) Model

- The least restrictive--used by Windows computers in small networks
- A subject has total control over any objects that he or she owns
- Along with the programs that are associated with those objects
- In the DAC model, a subject can also change the permissions for other subjects over objects

DAC Has Two Significant Weaknesses

- It relies on the end-user subject to set the proper level of security.
- A subject's permissions will be "inherited" by any programs that the subject executes.

User Account Control (UAC)



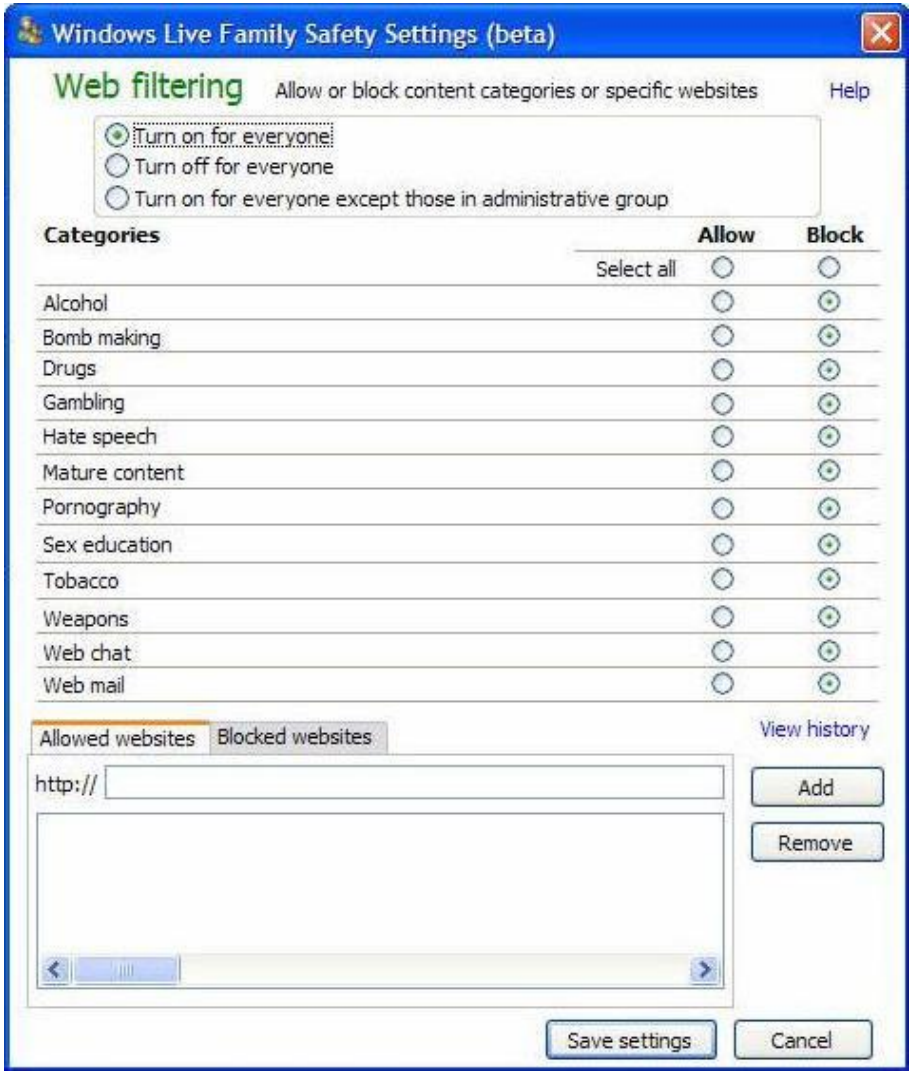
- Asks the user for permission when installing software
- Principle of **least privilege**
  - Users run with limited privileges by default
  - Applications run in standard user accounts
  - Standard users can perform common tasks

Role-Based Access Control (RBAC) Model

- Sometimes called **Non-Discretionary Access Control**
- Used in Windows corporate domains
- Considered a more “real world” approach than the other models
- Assigns permissions to particular roles in the organization, such as “Manager” and then assigns users to that role
- Objects are set to be a certain type, to which subjects with that particular role have access

Rule-Based Access Control (RBAC) Model

- Detailed Name: **Rule-Based Role-Based Access Control (RB-RBAC)** model or **automated provisioning**
- Controls access with **rules** defined by a custodian
  - *Example: Windows Live Family Safety*



Access Control Models Summary

Name	Restrictions	Description
Mandatory Access Control (MAC)	End user cannot set controls	Most restrictive model
Discretionary Access Control (DAC)	Subject has total control over objects	Least restrictive model
Role Based Access Control (RBAC)	Assigns permissions to particular roles in the organization and then users are assigned to roles	Considered a more "real world" approach
Rule Based Access Control (RBAC)	Dynamically assigns roles to subjects based on a set of rules defined by a custodian	Used for managing user access to one or more systems

Best Practices for Access Control

- **Separation of duties**
  - *No one person should control money or other essential resources alone*
    - Network administrators often have too much power and responsibility
- **Job rotation**
  - *Individuals are periodically moved from one job responsibility to another*

Best Practices for Access Control (Cont.)

- **Least privilege**
  - *Each user should be given only the minimal amount of privileges necessary to perform his or her job function*
- **Implicit deny**
  - *If a condition is not explicitly met, access is denied*
  - *For example, Web filters typically block unrated sites*

Trojan Horses (Software)

- A Trojan Horse is rogue software installed, perhaps unwittingly, by duly authorized users
- A Trojan Horse does what a user expects it to do, but in addition exploits the user's legitimate privileges to cause a security breach.
- Buggy Software Can Become Trojan Horse.
  - When a buggy software is exploited, it execute the code/intention of the attacker, while using the privileges of the user who started it

Questions?