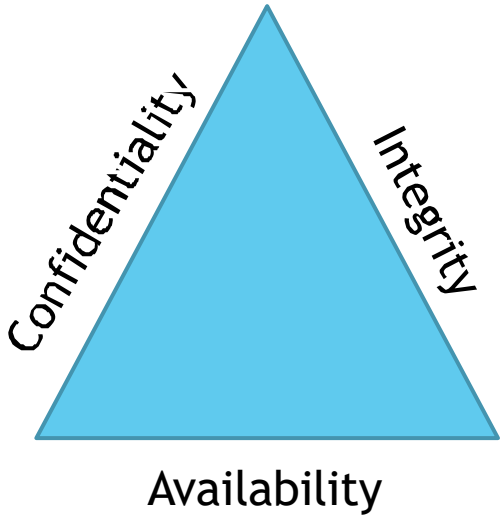
IA 313: Operating Systems Security

Lecture 1: ***Operating Systems Security Fundamentals***

What is a Secure System? (CIA Triad)

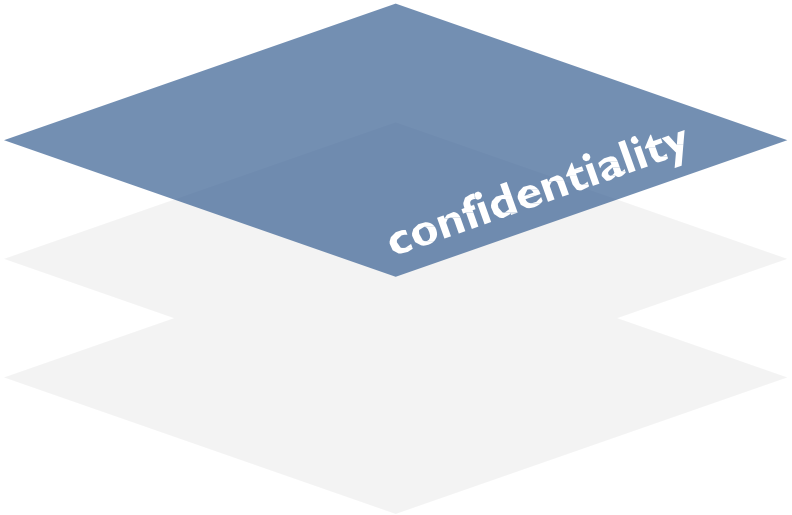


- ***Confidentiality*** – restrict access to authorized individuals
- ***Integrity*** – data has not been altered in an unauthorized manner
- ***Availability*** – information can be accessed and modified by authorized individuals in an appropriate timeframe

CIA Triad

Confidentiality

Protecting information from unauthorized access and disclosure

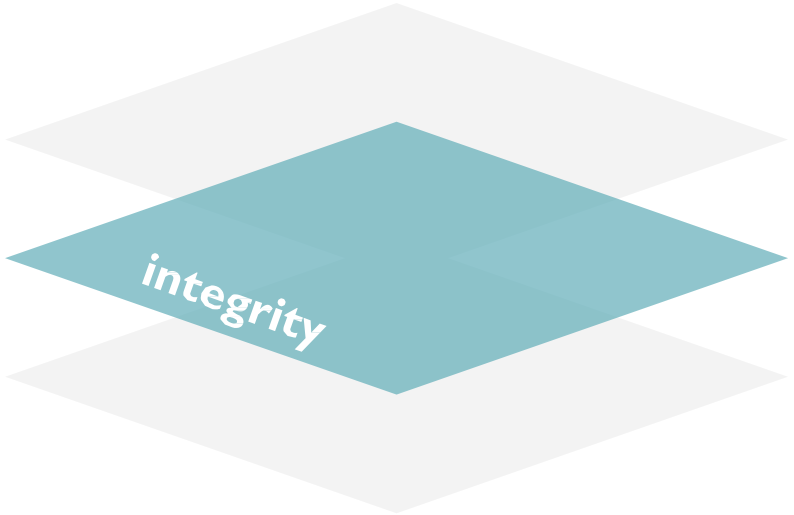


Example:
Criminal steals customers' usernames, passwords, or credit card information

CIA Triad …

Integrity

Protecting information from unauthorized modification

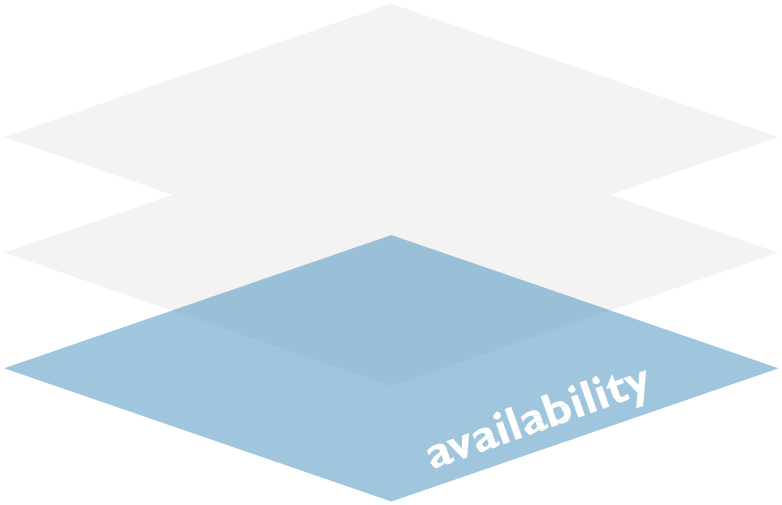


Example:
Someone alters payroll information or a proposed product design

CIA Triad …

Availability

Preventing disruption in how information is accessed



Example:

Your customers are unable to access your online services

Methods of Defense

- Five basic approaches to defense of computing systems
  - Prevent attack
    - Block attack / Close vulnerability
  - Deter attack
    - Make attack harder (can't make it impossible ☹)
  - Deflect attack
    - Make another target more attractive than this target
  - Detect attack
    - During or after
  - Recover from attack

What is operating system security?

- Is the process of ensuring OS integrity, confidentiality and availability.
- Refers to specified steps or measures used to protect the OS from threats, viruses, worms, malware or remote hacker intrusions.

What Security Goals Does Operating System Provide?

- Originally: time-sharing computers: enabling multiple users to securely share a computer
  - Separation and sharing of processes, memory, files, devices, etc.
- What is the threat model?
  - Users may be malicious, users have terminal access to computers, software may be malicious/buggy, and so on
- Security mechanisms
  - Memory protection
  - Processor modes
  - User authentication
  - File access control

What Security Goals Does Operating System Provide?

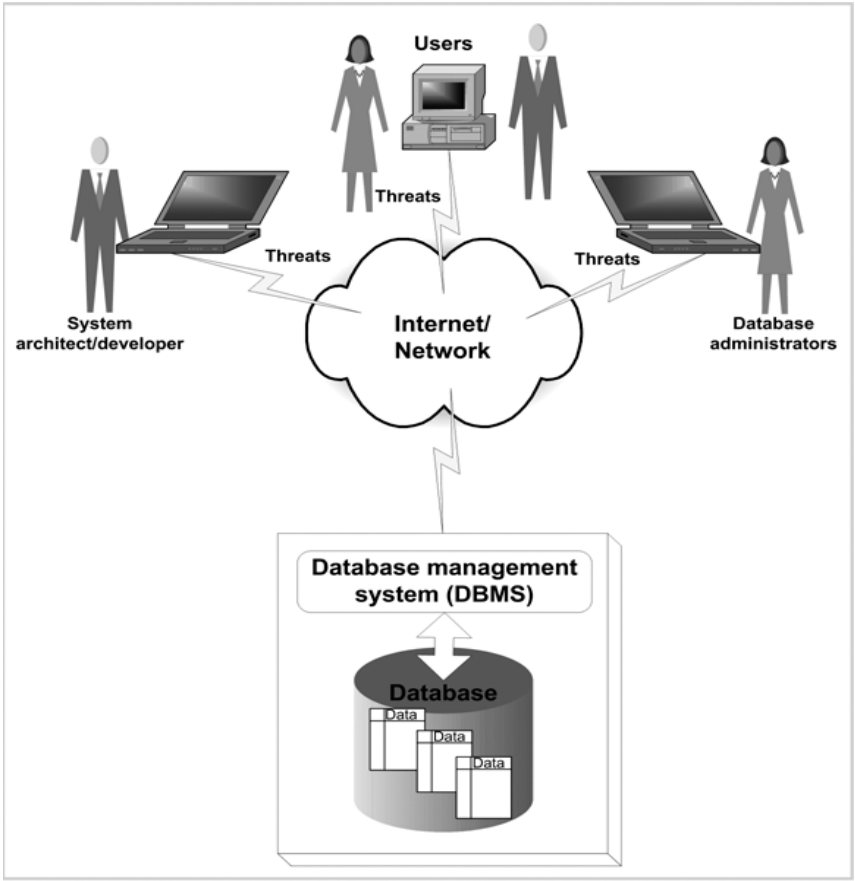
- More recent past and present: Networked desktop computers: ensure secure operation in networked environment
- New threat?
  - Attackers coming from the network. Network-facing programs on computers may be buggy. Users may be hurt via online communication.
- Security mechanisms
  - Authentication; Access Control
  - Secure Communication (using cryptography)
  - Logging & Auditing
  - Intrusion Prevention and Detection
  - Recovery

What Security Goals Does Operating System Provide?

- Present and near future: mobile computing devices:
- New threat?
  - Apps (programs) may be malicious.
  - More tightly connected with personal life of the owner.
- Security mechanisms?
  - Isolation of each app.
  - Help users assess risks of apps.
  - Risk communication.

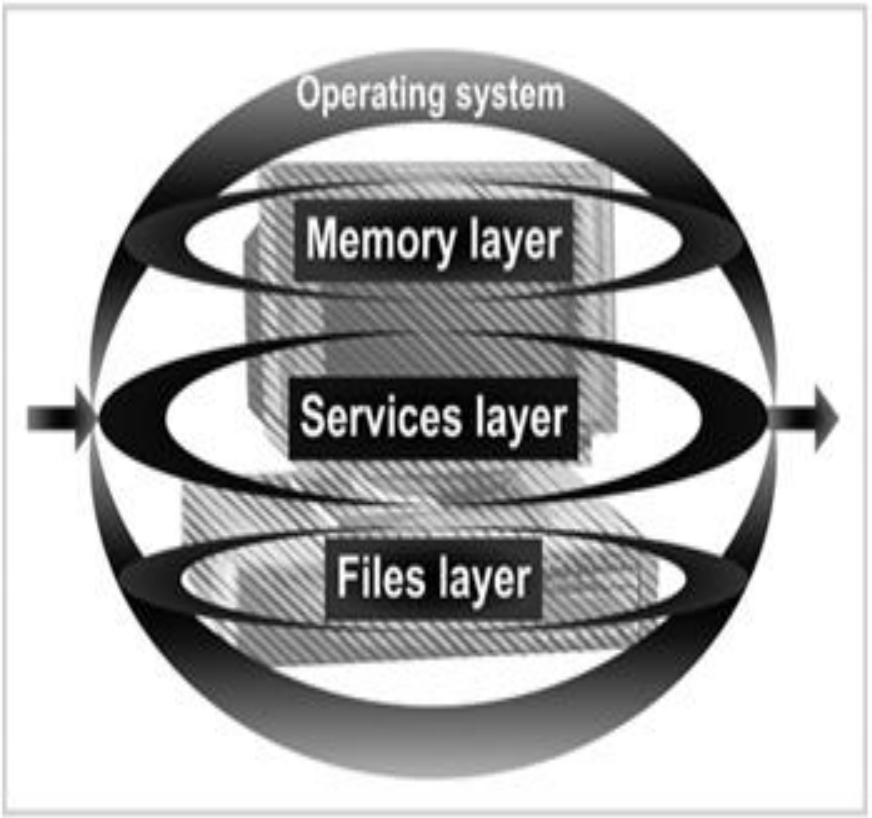
The OS Security Environment

- A compromised OS can compromise a database environment
- Physically protect the computer running the OS (padlocks, chain locks, guards, cameras)
- Model:
  - Bank building (operating system)
  - Safe (database)
  - Money (data)



The Components of an OS Security Environment

- Used as access points to the database
- Three components:
  - Services
  - Files
  - Memory



Services

- Main component of operating system security environment
- Used to gain access to the OS and its features
- Include
  - User authentication
  - Remote access
  - Administration tasks
  - Password policies

Authentication

- Method of proving the identity
  - Occurs when a control proves that a user possesses the identity that he or she claims
- How to prove an identity?
  - Something you know
  - Something you have
  - Something you are
- Use of passwords, token, or biometrics other private information
- What is two factor authentication?
  - Strong authentication

Authentication Methods

- Authentication:
  - Verifies user identity
  - Permits access to the operating system
- Physical authentication:
  - Allows physical entrance to company property
  - Magnetic cards and biometric measures
- Digital authentication: verifies user identity by digital means

Authentication Methods …

- Digital certificates: digital passport that identifies and verifies holder of certificate
- Digital token (security token):
  - Small electronic device
  - Displays a number unique to the token holder; used with the holder's PIN as a password
  - Uses a different password each time

Authentication Methods …

- Digital card:
  - Also known as a security card or smart card
  - Similar to a credit card; uses an electronic circuit instead of a magnetic strip
  - Stores user identification information
- Kerberos:
  - Developed by MIT
  - Uses tickets for authentication purposes

Authentication Methods …

- Lightweight Directory Access Protocol (LDAP):
  - Developed by the University of Michigan
  - A centralized directory database stores:
    - Users (user name and user ID)
    - Passwords
    - Internal telephone directory
    - Security keys
  - Efficient for reading but not suited for frequently changing information

Authentication Methods …

- NT LAN Manager (NTLM):
  - Developed and used by Microsoft
  - Employs a challenge/response authentication protocol
- Public Key Infrastructures (PKI):
  - User keeps a private key
  - Authentication firm holds a public key
  - Encrypt and decrypt data using both keys

Authentication Methods …

- RADIUS: used by network devices to provide a centralized authentication mechanism
- Secure Socket Layer (SSL): authentication information is transmitted over the network in an encrypted form
- Secure Remote Password (SRP):
  - Password is not stored locally
  - Invulnerable to brute force or dictionary attacks

Authorization

- Process that decides whether users are permitted to perform the functions they request
- Authorization is not performed until the user is authenticated
- Deals with privileges and rights

User Administration

- Create user accounts
- Set password policies
- Grant privileges to users
- Best practices:
  - Use a consistent naming convention
  - Always provide a password to an account and force the user to change it at the first logon
  - Protect passwords
  - Do not use default passwords

User Administration …

- Best practices …:
  - Create a specific file system for users
  - Educate users on how to select a password
  - Lock non-used accounts
  - Grant privileges on a per host basis
  - Do not grant privileges to all machines
  - Use ssh, scp, and Secure FTP
  - Isolate a system after a compromise
  - Perform random auditing procedures

Password Policies

- First line of defense
- Dictionary attack: permutation of words in dictionary
- Make hard for hackers entering your systems
- Best password policy:
  - Matches your company missions
  - Enforced at all level of the organization

Password Policies …

- Best practices:
  - Password aging
  - Password reuse
  - Password history
  - Password encryption
  - Password storage and protection
  - Password complexity
  - Logon retries
  - Single sign-on enables a user to log in once and gain access to the resources of multiple software systems without being prompted to log in again

Files

- Common threats:
  - File permission
  - File sharing
- Files must be protected from unauthorized reading and writing actions
- Data resides in files; protecting files protects data

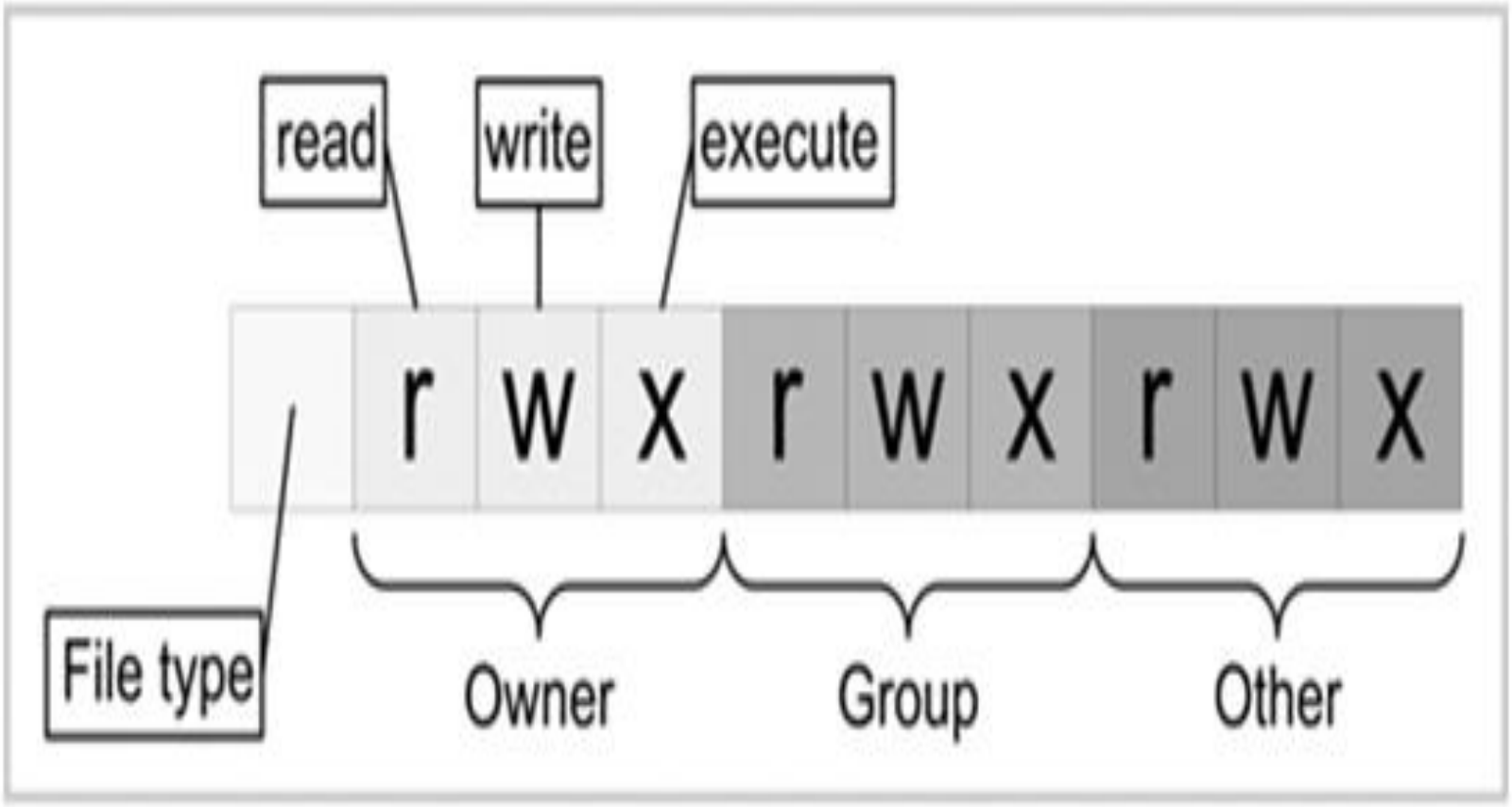
File Permissions

- Read, write, and execute privileges
- In Windows:
  - Change permission on the Security tab on a file's Properties dialog box
  - Allow indicates grant; Deny indicates revoke

File Permissions …

- In UNIX/Linux
  - Three permission settings: owner; group to which owner belongs; all other users
  - Each setting consist of rwx
    - r for reading, w for writing, and x for executing
  - CHMOD command used to change file permissions

File Permissions …




```
$ chmod  644  mail_list
```

File Transfer

- FTP (File Transfer Protocol):
  - Internet service for transferring files from one computer to another
  - Transmits usernames and passwords in plaintext
  - Root account cannot be used with FTP
  - Anonymous FTP: ability to log on to the FTP server without being authenticated

File Transfer …

- Best practices:
  - Use Secure FTP utility if possible
  - Make two FTP directories:
    - One for uploads with write permissions only
    - One for downloads with read permissions only
  - Use specific accounts with limited permissions
  - Log and scan FTP activities
  - Allow only authorized operations

Sharing Files

- Naturally leads to security risks and threats
- Peer-to-peer programs: allow users to share files over the Internet
- Reasons for blocking file sharing:
  - Malicious code
  - Adware and spyware
  - Privacy and confidentiality
  - Pornography
  - Copyright issues

Memory

- Hardware memory available on the system can be corrupted by badly written software
- Can harm data integrity
- Two options:
  - Stop using the program
  - Apply a patch (service pack) to fix it

Security Features of an Ordinary OS

- User identification and authentication
- File and I/O device access control
  - Table lookup of ACL matrix
- Memory protection
  - Usually preformed by hardware mechanisms, e.g., paging or segmentation
- Enforcement of sharing
  - Need to guarantee integrity and consistency
  - Table lookup combined with integrity control
- Guarantee of fair service
  - No starvation
  - Scheduling disciplines + hardware clocks
- Interprocess communication and synchronization
  - Mediated by access control tables.

Features of a Secure and Trusted OS

- Mandatory access control
  - Control policy made by central authority, not individual owner
  - E.g., military security
- Discretionary access control
  - Owner has certain amount of access control
  - Both MAC and DAC can be applied to the same object, MAC precedence over DAC
- Object reuse protection
  - Write over old data when file space is allocated
- Complete mediation
  - Prevent any access that circumvents monitor
  - All access are checked (sandboxing)
- Accountability and Audit
- Intrusion detection

Security Kernel

- **Kernel** is the lowest-level part of the OS
- Kernel is responsible for
  - Synchronization
  - Inter-process communication
  - Message passing
  - Interrupt handling
- The **security kernel** is the part of the kernel that deals with security
- Security kernel contained within the kernel

Security Kernel …

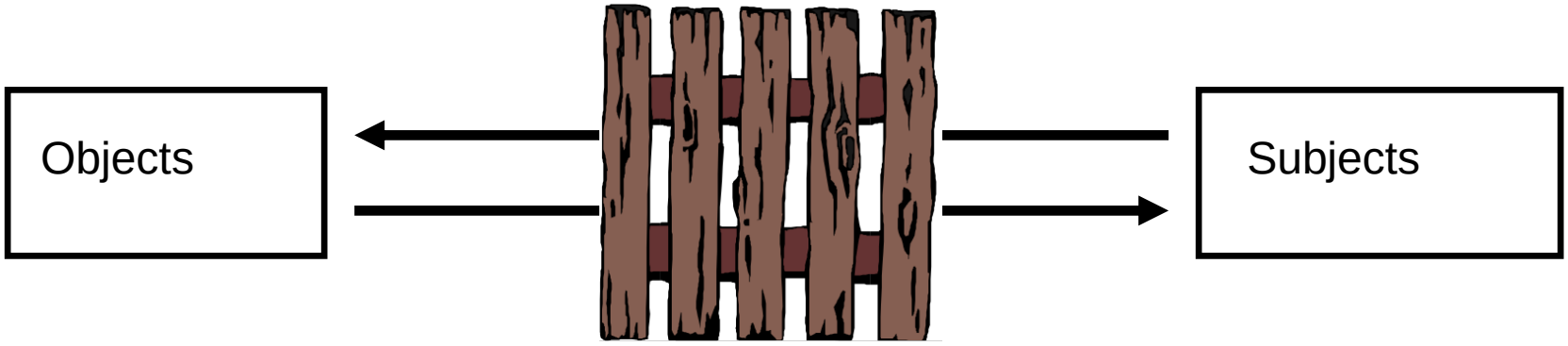
- Why have a security kernel?
- All accesses go thru kernel
  - Ideal place for access control
- Security-critical functions in one location
  - Easier to analyze and test
  - Easier to modify
- More difficult for attacker to get in “below” security functions

Principles of Security Kernel

- Coverage – of each access
- Separation – of security functions from rest
- Unity – a single module
- Modifiability and Maintenance – easy to control
- Compactness – small and therefore verifiable

Reference Monitor

- The part of the security kernel that deals with access control
  - Mediates access of subjects to objects
  - Tamper-resistant
  - Analyzable (small, simple, etc.)

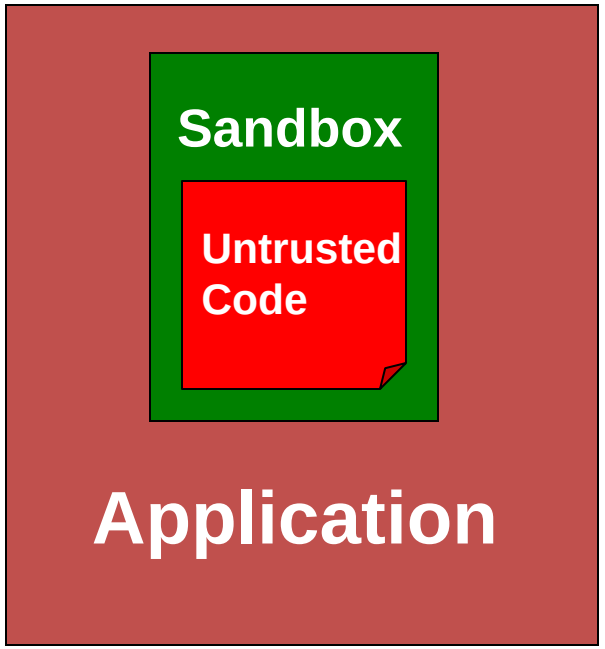


Audit

- Log security-related events
- Protect audit log
  - Write to write-once non-volatile medium
- Audit logs can become huge
  - Simplifying auditing
    - Audit only first, last access by process to a file
    - Do not record routine, expected events
      - E.g., starting one process always loads …
  - Audit reduction still a big problem

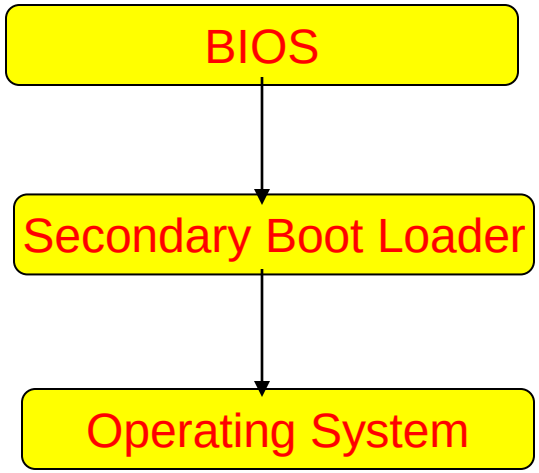
Sandboxing

- Run code in limited environment
- Verify each system call
- Verify each memory reference
- Advantage
  - Fine-grained control
- Disadvantages
  - Efficiency
  - Expressing security policy
  - Sandbox may have security vulnerabilities



Booting Sequence and Security

- Typical booting sequence is



There is a chain of trust in booting process

An attacker can subvert booting process by altering or modifying something in any of these components

In order to protect system from such changes most systems have a BIOS password

Hibernation and Security

- Hibernation is a concept of saving state of system into disk
  - Typically in a file state information is stored
  - Entire main memory is copied into a file (in a compressed format)
- Since entire state is copied onto disk
  - All passwords and other sensitive information carry danger of being exposed
- Researchers have shown the feasibility of extracting such information by mounting a live CD attack
- On a windows machine state is stored in a file c:\hiberfil.sys