CSE321 Assignment 3: System Protection Mechanisms

SECCOMP (Secure Computing Mode)

Basic Idea:

SECCOMP is a Linux feature that limits the system calls a program can use. It helps reduce the risk if a program is attacked. There are two modes, one is strict .It only allows a few calls like read, write, exit, and sigreturn. The other uses filters to allow only selected calls.

Use Cases:

Sandboxing untrusted programs like browsers or PDF viewers.
It is used in Docker containers to limit actions inside the container.
It is also used in system services to increase security.

SELinux (Security-Enhanced Linux)

Basic Idea:

SELinux is a strong security system that controls what users and processes can do. It uses labels and rules to decide what actions are allowed. Even root users can be limited if the policy does not allow them.

Use Cases:

It is used in servers and government systems for strict access control.
It Helps prevent apps from accessing files or processes they should not..
It is also good for multi-user systems with sensitive data.

chroot (Change Root)

Basic Idea:

The chroot command changes the root directory for a process. After using chroot, the process cannot access files outside the new root. It creates a jail-like environment. However, it is not very secure because if a process gets root access, it can escape.

Use Cases:

Running older software in a safe environment.

Creating simple isolated environments for testing.
Used by some servers like FTP to limit user access.

Comparison

Feature	SECCOMP	SELinux	chroot
Security Type	Syscall filtering	Mandatory Access Control (MAC)	Filesystem isolation
Kernel Support	Yes (Linux kernel >= 2.6.12)	Yes (Integrated in Linux kernel)	Yes (Linux/Unix)
Root Bypass?	No	No	Yes (can be bypassed by root)
Ease of Use	Medium (requires programming)	Complex (requires policy management)	Easy
Performance	High efficiency (low overhead)	Moderate (depends on policies)	High efficiency
Use in Docker	Yes (used in profiles)	Optional (can be enabled)	Not commonly used
Best for	Limiting program syscalls	Enterprise-level access control	Simple filesystem isolation