User Command Sandbox: Policy Requirements Document

Teaching Assistant
E0256 - Computer Systems Security
Indian Institute of Science

Autumn 2025

1 Introduction

This document specifies the mandatory policy requirements for the User Command Sandbox project. All student implementations must enforce these policies at the kernel level for the `curl` command. The policies are designed to demonstrate the advantages of kernel-level enforcement over container-based approaches, providing fine-grained control over system resources and security boundaries.

2 Policy Categories and Requirements

2.1 Network Access Policies

Table 1: Network Access Policy Requirements

Policy ID	**Policy Description**	**Enforcement Level**
NET-001	Allow HTTP/HTTPS connections only to domains specified in whitelist	BLOCK
NET-002	Block all FTP, SFTP, and other non-HTTP protocols	BLOCK
NET-003	Restrict maximum connection duration to 30 seconds	TIMEOUT
NET-004	Limit concurrent connections to 3 simultaneous connections	THROTTLE
NET-005	Block connections to private IP ranges (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)	BLOCK
NET-006	Allow only ports 80 (HTTP) and 443 (HTTPS)	BLOCK

2.2 File System Policies

Table 2: File System Access Policy Requirements

Policy ID	Policy Description	Enforcement Level
FS-001	Allow file writes only to `/tmp/curl_downloads/` directory	RESTRICT
FS-002	Block all file read operations outside user's home directory	BLOCK
FS-003	Maximum file download size: 10MB per file	QUOTA
FS-004	Prevent execution of downloaded files	BLOCK
FS-005	Restrict total storage usage to 50MB	QUOTA
FS-006	Block access to system directories (`/etc/`, `/bin/`, `/sbin/`, `/usr/`)	BLOCK

2.3 Memory and Process Policies

Table 3: Memory and Process Policy Requirements

Policy ID	Policy Description	Enforcement Level
MEM-001	Maximum memory usage: 100MB	LIMIT
MEM-002	Prevent fork() and exec() system calls during execution	BLOCK
MEM-003	Maximum process execution time: 2 minutes	TIMEOUT
MEM-004	Restrict CPU usage to 50% of single core	THROTTLE
MEM-005	Block memory mapping of executable pages	BLOCK
MEM-006	Limit stack size to 8MB	LIMIT

2.4 Security and Isolation Policies

3 Policy Configuration Format

Students must implement policy configuration using JSON (or any other suitable file format) as shown below:

```
{
  "policy_version": "1.0",
  "command": "curl",
  "network_policies": {
    "allowed_domains": ["example.com", "iisc.ac.in", "trusted.org"],
```

Table 4: Security and Isolation Policy Requirements

Policy ID	Policy Description	Enforcement Level
SEC-001	Run curl as non-privileged user (nobody)	ISOLATE
SEC-002	Block access to environment variables containing ”PASSWORD”, ”KEY”, ”SECRET”	FILTER
SEC-003	Prevent network interface configuration changes	BLOCK
SEC-004	Restrict signal handling (allow only TERM, INT)	FILTER
SEC-005	Block access to kernel memory and modules	BLOCK
SEC-006	Isolate network namespace from host	ISOLATE

```
    "allowed_ports": [80, 443],
    "max_connections": 3,
    "connection_timeout": 30,
    "block_private_ips": true
  },
  "filesystem_policies": {
    "allowed_write_dirs": ["/tmp/curl_downloads/"],
    "max_file_size": 10485760,
    "max_total_storage": 52428800,
    "blocked_paths": ["/etc/", "/bin/", "/sbin/", "/usr/"]
  },
  "memory_policies": {
    "max_memory": 104857600,
    "max_stack_size": 8388608,
    "max_cpu_time": 120,
    "cpu_limit_percent": 50
  },
  "security_policies": {
    "run_as_user": "nobody",
    "blocked_environment": ["PASSWORD", "KEY", "SECRET"],
    "allowed_signals": ["TERM", "INT"],
    "isolate_network": true
  }
}
```

4 Enforcement Mechanisms

4.1 System Call Interception

Students must implement system call interception for the following critical operations:

- **Socket operations:** socket(), connect(), bind(), accept()

- **File operations:** open(), openat(), read(), write(), mkdir()
- **Process operations:** fork(), execve(), clone()
- **Memory operations:** mmap(), brk(), mprotect()
- **Signal operations:** signal(), sigaction()

4.2 Policy Violation Handling

Table 5: Policy Violation Response Requirements

Violation Type	**Required Action**	**Log Message**
Network Policy Violation	Block connection + Terminate process	"NETWORK_VIOLATION: Attempted connection to blocked domain"
File System Violation	Block operation + Continue execution	"FS_VIOLATION: Attempted write to restricted path"
Memory Limit Exceeded	Terminate process + Cleanup	"MEMORY_VIOLATION: Exceeded allocated memory limit"
Timeout Violation	Terminate process	"TIMEOUT_VIOLATION: Process exceeded maximum execution time"
Security Violation	Immediate termination	"SECURITY_VIOLATION: Attempted privileged operation"

5 Testing and Validation Requirements

5.1 Mandatory Test Cases

Students must demonstrate the following test scenarios:

1. **Test NET-001:** Attempt to connect to non-whitelisted domain → Should be blocked
2. **Test NET-005:** Attempt to connect to 192.168.1.1 → Should be blocked
3. **Test FS-001:** Attempt to write to `/home/user/file` → Should be blocked
4. **Test FS-003:** Download file larger than 10MB → Should be blocked
5. **Test MEM-001:** Allocate 150MB memory → Process should be terminated

6. **Test MEM-003:** Run process for 3 minutes → Should timeout and terminate
7. **Test SEC-002:** Access environment variable with "PASSWORD" → Should be filtered

6 Evaluation Criteria

6.1 Policy Implementation (40%)

- Complete implementation of all mandatory policies (20%)
- Correct handling of policy violations (10%) Policy configuration parsing and application (10%)

6.2 Security Effectiveness (30%)

- Successful prevention of all policy violations (15%)
- Proper isolation from host system (10%)
- Secure cleanup after termination (5%)

6.3 Code Quality and Documentation (30%)

- Clean, well-documented kernel module/eBPF code (15%)
- Comprehensive test suite coverage (10%)
- Clear architecture documentation (5%)