

CS 628A: Computer Systems Security

MODULE 2: SECURITY OF PROGRAM EXECUTION AND SYSTEM SECURITY

Isolation and Confinement

Pramod Subramanyan

Acknowledgements

- Sandeep Shukla (IIT Kanpur)
- Dan Boneh (Stanford University)
- John C. Mitchell (Stanford University)
- Nicolai Zeldovich (MIT)
- Jungmin Park (Virginia Tech)
- Patrick Schaumont (Virginia Tech)
- C. Edward Chow
- Arun Hodigere
- Web Resources

Three Types of Security Policies

- Confidentiality
- Integrity
- Availability

Information flow policies

Sometimes called the CIA triad

[Anderson, 1972] [Saltzer and Schroeder, 1975]


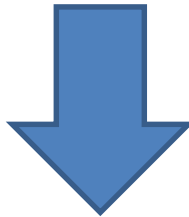
Goals of Confidentiality Policies

Prevent unauthorized disclosure of info

- Example: Privacy Act requires that certain personal data be kept confidential. E.g., income tax return info only available to IT department and legal authority with court order. It limits the distribution of documents/info
- Other examples from US: FERPA, HIPPA

How does access control work?

```
int *ptr = 0x12345678;  
*ptr = 0xcafef00d;
```



```
mov rbx, 0x12345678    // get addr  
mov [rbx], 0xcafef00d // store
```

Processor starts executing page fault handler now

How does access control work?

- TLB lookup fails
 - Processor walks page table
- Page walk also fails to return valid translation
 - Processor starts executing page fault handler (OS)
- OS again walks the page table (why?)
 - Finds page is not mapped to application
 - Two things can happen: map page, or signal app
 - Signal can be handled or application killed

Discretionary Access Control (DAC)

- Mechanism where **user** can set controls to allow/deny access to an object
- Also called Identity-based access control (IBAC)
- Traditional access control technique implemented by traditional operating systems such as Unix.
 - Based on user identity and ownership
 - Programs run by user inherit all privileges granted to user
 - Programs is free to change access to user's objects
 - Support only two major categories of users: completely trusted admins and completely untrusted ordinary users

Problems with DAC (1/3)

- Each users has complete discretion over his objects.
 - What is wrong with that?
 - Difficult to enforce a system-wide security policy
 - A user can leak classified documents to a unclassified users.

Problems with DAC (2/3)

- Only based on user's identity and ownership, ignoring relevant info such as
 - User's role
 - Function of the program
 - Trustworthiness of the program
 - Compromised prog can change access to user's objects
 - Compromised prog inherits all the permissions granted to the users (especially the root user)
 - Sensitivity of the data
 - Integrity of the data

Problems with DAC (3/3)

- Only support coarse-grained privileges
- Unbounded privilege escalation
- Too simple classification of users (How about more than two categories of users?)

Mandatory Access Control (MAC)

- Mechanism where system control access to an object and a user cannot alter that access.
- Defined by three major properties:
 - Administratively-defined security policy
 - Control over all subjects (process) and objects (files, sockets, network interfaces)
 - Decisions based on all security-relevant info
- MAC access decisions are based on labels that contains security-relevant info

Example: SELinux

What Can MAC Offer?

- Supports wide variety of categories of users
- Strong separation of security domains
- System, application, and data integrity
- Ability to limit program privileges
 - Confine damage due to flawed/malicious software
- Authorization limits for legitimate users

ISOLATION

THE CONFINEMENT PRINCIPLE

Running untrusted code

We often need to run buggy/untrusted code:

- programs from untrusted Internet sites:
 - apps, extensions, plug-ins, codecs for media player
- exposed applications: pdf viewers, outlook
- honeypots

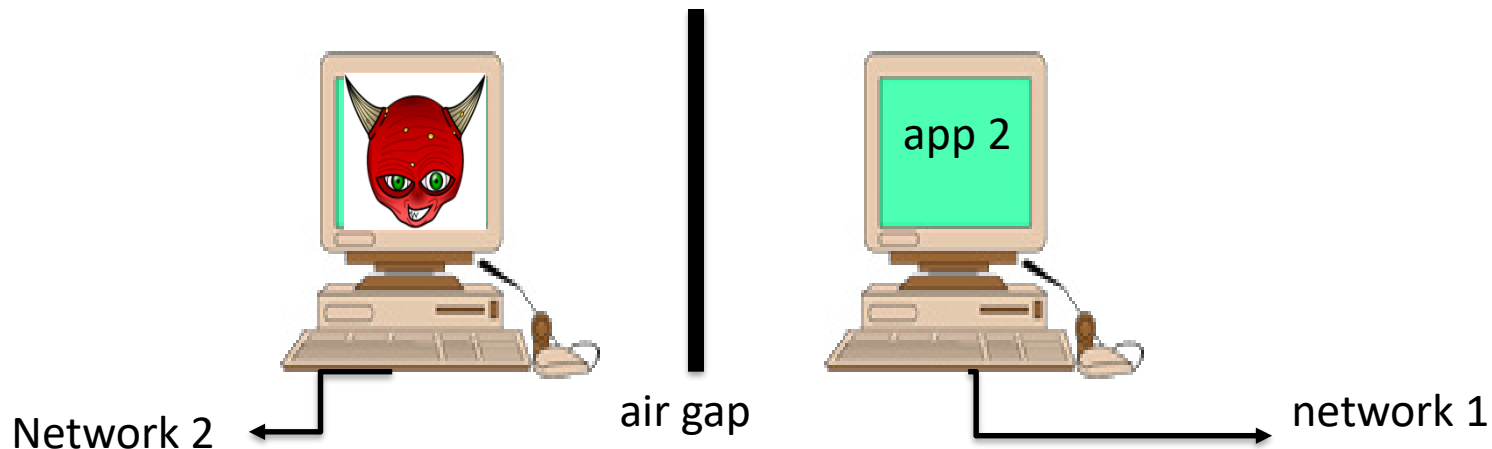
Goal: if application “misbehaves” \Rightarrow **kill it**

Approach: confinement

Confinement: Ensure misbehaving app cannot harm rest of system

Can be implemented at many levels:

- **Hardware**: run application on isolated hw (air gap)



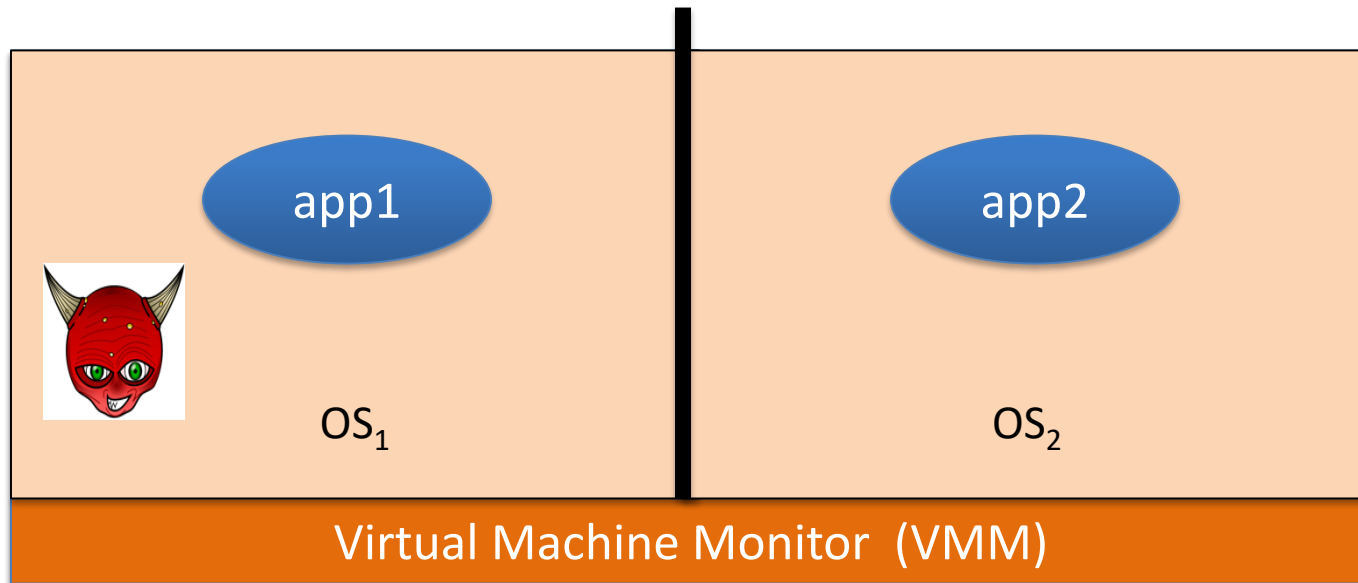
Resource Expensive

Approach: confinement

Confinement: ensure misbehaving app cannot harm rest of system

Can be implemented at many levels:

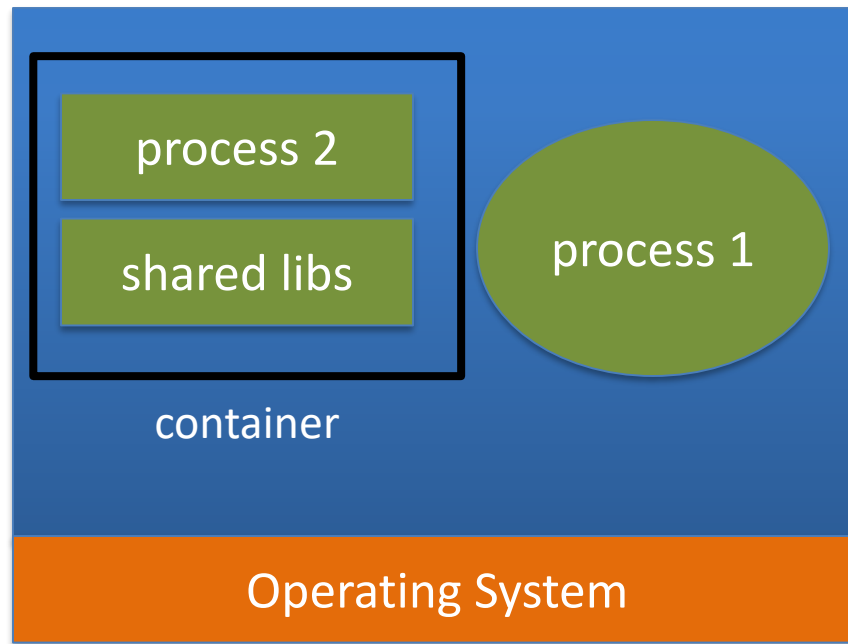
- **Virtual machines**: isolate OS's on a single machine



Approach: confinement

Confinement: Create a **lightweight container** for each application

- **Container:** Has process + all libraries needed for it
- Users inside container may have more rights than outside

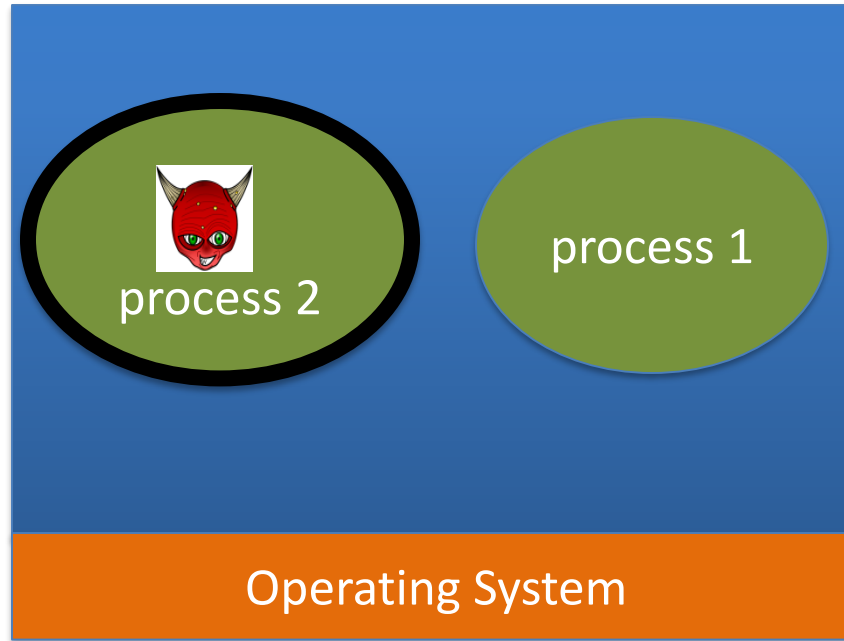


Approach: confinement

Confinement: Ensure misbehaving app cannot harm rest of system

Can be implemented at many levels:

- **Process:** System Call Interposition
Isolate a process in a single operating system



Approach: confinement

Confinement: ensure misbehaving app cannot harm rest of system

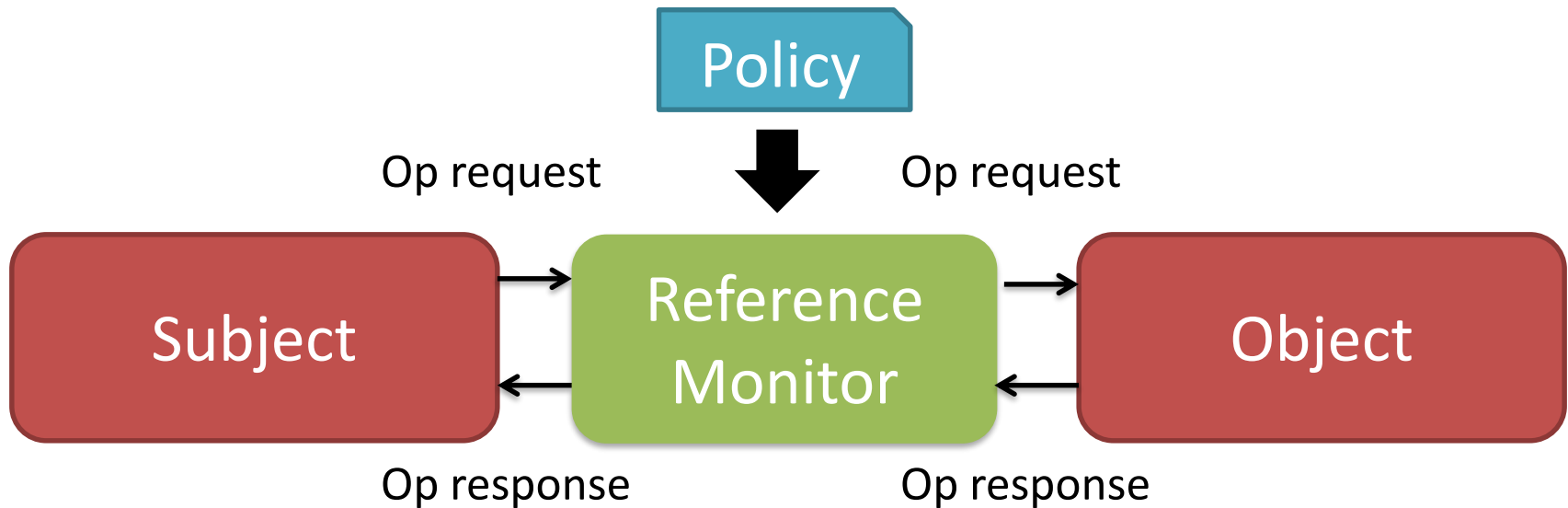
Can be implemented at many levels:

- **Threads:** Software Fault Isolation (SFI)
 - Isolating threads sharing same address space
 - Thread Local Storage (TLS)
- **Application:** e.g. browser-based confinement
 - Discretionary Access Control
 - SOP – Same Origin Policy
 - CSP – Content Security Policy
 - CORS – Cross Origin Resource Sharing
 - Mandatory Access Control
 - COWL – Confinement with Original Web Label

Implementing confinement

Key component: **reference monitor**

- **Mediates requests** from applications
 - Implements protection policy
 - Enforces isolation and confinement
- Must **always** be invoked:
 - Every application request must be mediated
- **Tamperproof:**
 - Reference monitor cannot be killed
 - ... or if killed, then monitored process is killed too
- **Small** enough to be analyzed and validated



Principles:

1. **Complete Mediation:** monitor must always be invoked
2. **Tamper-proof:** monitor cannot be changed by adversary
3. **Verifiable:** reference monitor is small enough to thoroughly understand, test, and ultimately, verify.

Reference Monitors in Practice

- Who is mediating what?
 - For isolation through VMs
 - For isolation through containers
 - For isolation through system call interposition
- How do we ensure complete mediation?
- How do we ensure tamper proofing?

A Detour

- A few words about Unix User IDs and IDs associated with Unix Processes

Source: CS426 Course at Purdue Univ.

Principals and Subjects

- A subject is a program (application) executing on behalf of some principal(s)
- A principal may at any time be idle, or have one or more subjects executing on its behalf

What are subjects in UNIX?

What are principals in UNIX?

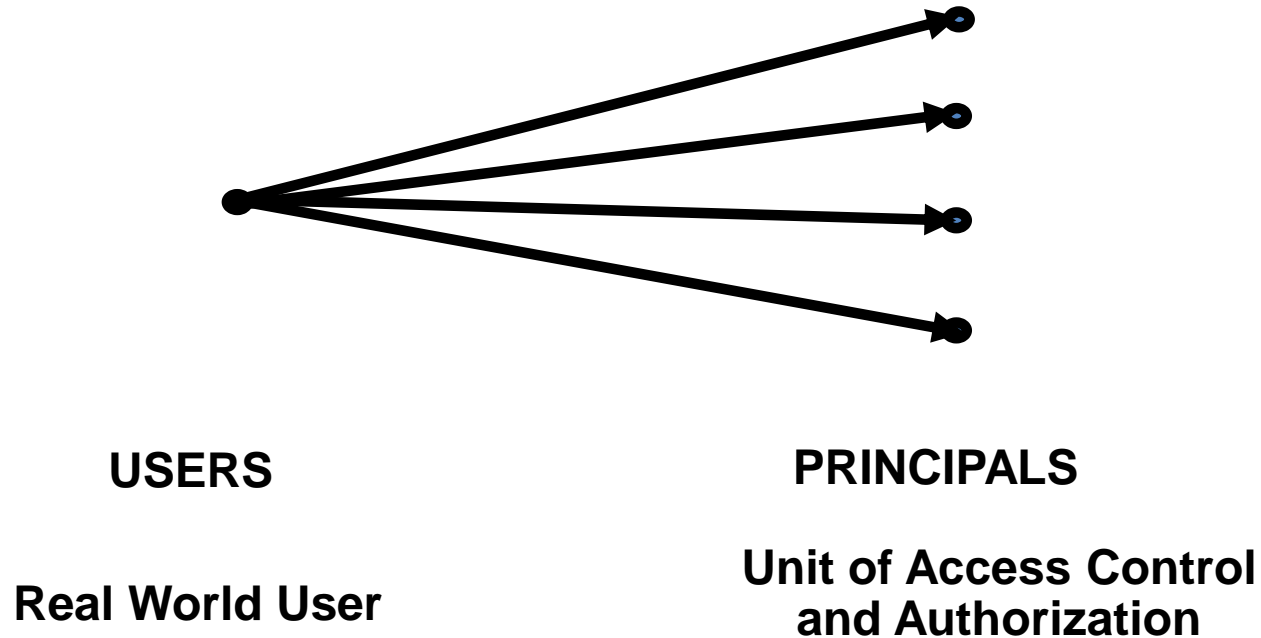
Objects

- An object is anything on which a subject can perform operations (mediated by rights)
- Usually objects are passive, for example:
 - File
 - Directory (or Folder)
 - Memory segment
- But, subjects can also be objects, with operations
 - kill
 - suspend
 - resume

Basic Concepts of UNIX Access Control: Users, Groups, Files, Processes

- Each user account has a unique UID
 - The UID 0 means the super user (system admin)
- A user account belongs to multiple groups
- Subjects are processes
 - associated with uid/gid pairs, e.g., (euid, egid), (ruid, rgid), (suid, sgid)
- Objects are files

Users and Principals



the system authenticates the human user to a particular principal

Users and Principals

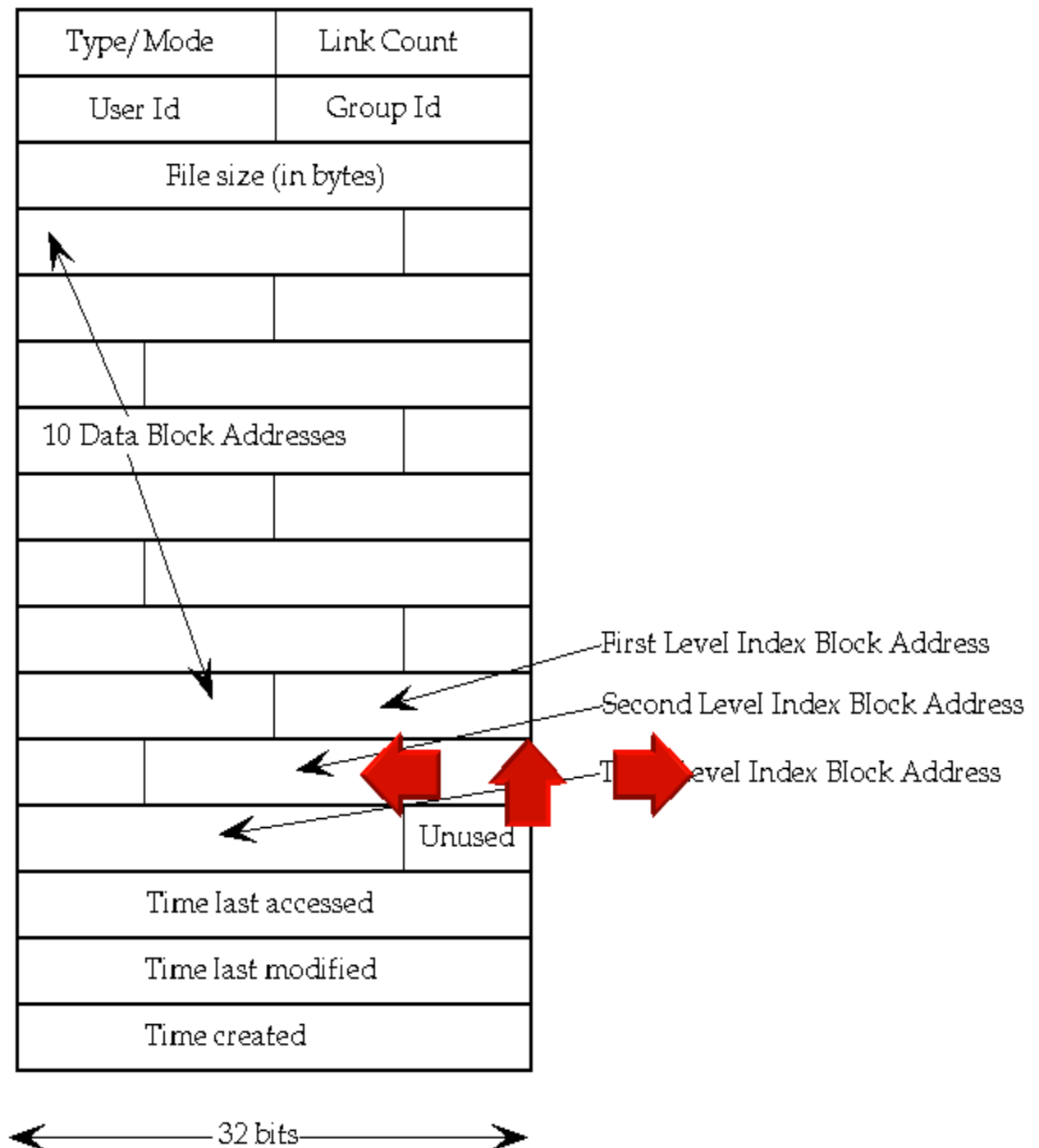
- There should be a one-to-many mapping from users to principals
 - a user may have many principals, but
 - each principal is associated with an unique user
- This ensures accountability of a user's actions

What does the above imply in UNIX?

Organization of Objects

- Almost all objects are modeled as files
 - Files are arranged in a hierarchy
 - Files exist in directories
 - Directories are also one kind of files
- Each object has
 - owner
 - group
 - 12 permission bits
 - rwx for owner, rwx for group, and rwx for others
 - suid, sgid, sticky

UNIX inodes: Each file corresponds to an inode



Basic Permissions Bits on Files

- Read controls reading the content of a file
 - i.e., the read system call
- Write controls changing the content of a file
 - i.e., the write system call
- Execute controls loading the file in memory and execute
 - i.e., the execve system call

Execution of a file

- Binary file vs. script file
- Having execute but not read, can one run a binary file?
- Having execute but not read, can one run a script file?
- Having read but not execute, can one run a script file?

Permission Bits on Directories

- Read bit allows one to show file names in a directory
- The execution bit controls traversing a directory
 - does a lookup, allows one to find inode # from file name
 - `chdir` to a directory requires execution
- Write + execution control creating/deleting files in the directory
 - Deleting a file under a directory requires no permission on the file
- Accessing a file identified by a path name requires execution to all directories along the path

The suid, sgid, sticky bits

	suid	sgid	sticky bit
non-executable files	no effect	affect locking (unimportant for us)	not used anymore
executable files	change euid when executing the file	change egid when executing the file	not used anymore
directories	no effect	new files inherit group of the directory	only the owner of a file can delete

Some Examples

- What permissions are needed to access a file/directory?
 - read a file: /d1/d2/f3
 - write a file: /d1/d2/f3
 - delete a file: /d1/d2/f3
 - rename a file: from /d1/d2/f3 to /d1/d2/f4
 - ...
- File/Directory Access Control is by System Calls
 - e.g., open(2), stat(2), read(2), write(2), chmod(2), opendir(2), readdir(2), readlink(2), chdir(2), ...

The Three sets of permission bits

- Intuition:
 - if the user is the owner of a file, then the r/w/x bits for owner apply
 - otherwise, if the user belongs to the group the file belongs to, then the r/w/x bits for group apply
 - otherwise, the r/w/x bits for others apply
- Can one implement negative authorization, i.e., only members of a particular group are not allowed to access a file?

Other Issues On Objects in UNIX

- Accesses other than read/write/execute
 - Who can change the permission bits?
 - The owner can
 - Who can change the owner?
 - Only the superuser (why?)
- Rights not related to a file
 - Affecting another process
 - Operations such as shutting down the system, mounting a new file system, listening on a low port
 - traditionally reserved for the root user

Subjects vs. Principals

- Access rights are specified for users (accounts)
- Accesses performed by processes (subjects)
- The OS needs to know on which users' behalf a process is executing

Process User ID Model in Modern UNIX Systems

- Each process has three user IDs
 - real user ID (ruid) owner of the process
 - effective user ID (euid) used in most access control decisions
 - saved user ID (suid)
- and three group IDs
 - real group ID
 - effective group ID
 - saved group ID

Process User ID Model in Modern UNIX Systems

- When a process is created by *fork*
 - it inherits all three users IDs from its parent process
- When a process executes a file by *exec*
 - it keeps its three user IDs unless the set-user-ID bit of the file is set, in which case the effective uid and saved uid are assigned the user ID of the owner of the file
- A process may change user ids via system calls

The Need for suid/sgid Bits

- Some operations are not modeled as files and require user id = 0
 - halting the system
 - bind/listen on “privileged ports” (TCP/UDP ports below 1024)
 - non-root users need these privileges
- File level access control is not fine-grained enough
- System integrity requires more than controlling who can write, but also how it is written

What's the deal with passwords?

- Does the kernel store passwords? **NO!**
 - Where are they stored?
 - /etc/passwd and /etc/shadow
 - Who checks them?
 - An app with setuid bit set checks them
 - It's just a hash a with salt
- ```
$ mkpasswd -msha-512 <passwd> <salt>
```

# What does sudo do?

- Runs a command as root or a specified user
- How does it work?
  - Setuid bit is set on /usr/bin/sudo
  - Runs fork() and then execve()
- Why does sudo ask for the password?
- Will it work without setuid bit?
- Why is it better than logging in as root?
- Impact of buffer overflow in sudo?

# Security Problems of suid/sgid

- These programs are typically setuid root
- Violates the least privilege principle
  - every program and every user should operate using least privilege necessary to complete the job
- Why violating least privilege is bad?
- How would an attacker exploit this problem?
- How to solve this problem?

# Changing effective user IDs

- A process that executes a set-uid program can drop its privilege; it can
  - drop privilege permanently
    - removes the privileged user id from all three user IDs
  - drop privilege temporarily
    - removes the privileged user ID from its effective uid but stores it in its saved uid, later the process may restore privilege by restoring privileged user ID in its effective uid

# Access Control in Early UNIX

- A process has two user IDs: real uid and effective uid and one system call `setuid`
  - The system call `setuid(id)`
    - when `uid` is 0, `setuid` set both the `ruid` and the `eu` to the parameter
    - otherwise, the `setuid` could only set effective uid to real uid
      - Permanently drops privileges
  - A process cannot temporarily drop privilege
- Setuid Demystified, In USENIX Security '02

# System V

- Added saved uid & a new system call
- The system call seteuid
  - if euid is 0, seteuid could set euid to any user ID
  - otherwise, could set euid to ruid or suid
    - Setting to ruid temporarily drops privilege
- The system call setuid is also changed
  - if euid is 0, setuid functions as seteuid
  - otherwise, setuid sets all three user IDs to real uid

# BSD

- Uses ruid & euid, change the system call from setuid to setreuid
  - if euid is 0, then the ruid and euid could be set to any user ID
  - otherwise, either the ruid or the euid could be set to value of the other one
    - enables a process to swap ruid & euid



# Modern UNIX

- System V & BSD affect each other, both implemented `setuid`, `seteuid`, `setreuid`, with different semantics
  - some modern UNIX introduced `setresuid`
- Messy, complicated, inconsistent, and buggy
  - POSIX standard, Solaris, FreeBSD, Linux
  - Linux introduced an `fsuid` as well
  - Bug in Linux led to `fsuid = 0` even after dropping other privileges

# Readings for This Lecture

- Wiki
  - [Filesystem Permissions](#)
- Other readings
  - UNIX File and Directory Permissions and Modes
    - <http://www.hccfl.edu/pollock/AUunix1/FilePermissions.htm>
  - Unix file permissions
    - <http://www.unix.com/tips-tutorials/19060-unix-file-permissions.html>



# An old example: chroot

Often used for “guest” accounts on ftp sites

To use do: (must be root)

```
chroot /tmp/guest
su guest
```

root dir “/” is now “/tmp/guest”  
EUID set to “guest”

Now “/tmp/guest” is added to file system accesses for applications in jail

**open(“/etc/passwd”, “r”) ⇒**

**open(“/tmp/guest/etc/passwd”, “r”)**

⇒ application cannot access files outside of jail

# Jailkit

Problem: all utility progs (ls, ps, vi) must live inside jail

- **jailkit** project: auto builds files, libs, and dirs needed in jail env
  - **jk\_init**: creates jail environment
  - **jk\_check**: checks jail env for security problems
    - checks for any modified programs,
    - checks for world writable directories, etc.
  - **jk\_lsh**: restricted shell to be used inside jail
- **note**: simple chroot jail does not limit network access

```
$ wget http://olivier.sessink.nl/jailkit/jailkit-2.19.tar.gz
```

```
$ gunzip jailkit-2.19.tar.gz
```

```
$ tar xvf jailkit-2.19.tar
```

```
$ cd jailkit-2.19
```

```
$./configure
```

```
$ make
```

```
$ make install
```

# Escaping from jails

Early escapes: relative paths

`open( "../etc/passwd", "r" ) ⇒`

`open( "/tmp/guest/../../etc/passwd", "r" )`

**chroot** should only be executable by root.

---

– otherwise jailed app can do:

- create dummy file `"/aaa/etc/passwd"`
- `echo root::0:0:::/:/bin/sh > /aaa/etc/passwd`
- `mkdir /aaa/bin`
- `cp /bin/sh /aaa/bin`
- **run chroot `"/aaa"`**
- run `su root` to become root (bug in Ultrix 4.0)

```

#include <unistd.h>
#include <stdlib.h>
#include <stdio.h>
#include <fcntl.h>
#include <sys/types.h>
#include <sys/stat.h>

void die(char *msg) {
 perror(msg);
 exit(1);
}

int main(int argc, char *argv[])
{
 int i, fd;

 if (chdir("/") != 0)
 die("chdir(/)");

 if ((fd = open("/", O_RDONLY)) == -1)
 die("open(/)");

 if (mkdir("baz", 0777) != 0)
 die("mkdir(baz)");

 if (chroot("baz") != 0)
 die("chroot(baz)");

 if (fchdir(fd) == -1)
 die("fchdir");

 if (chroot(".") != 0)
 die("chroot(.)");

 printf("Exploit seems to work. =)\n");

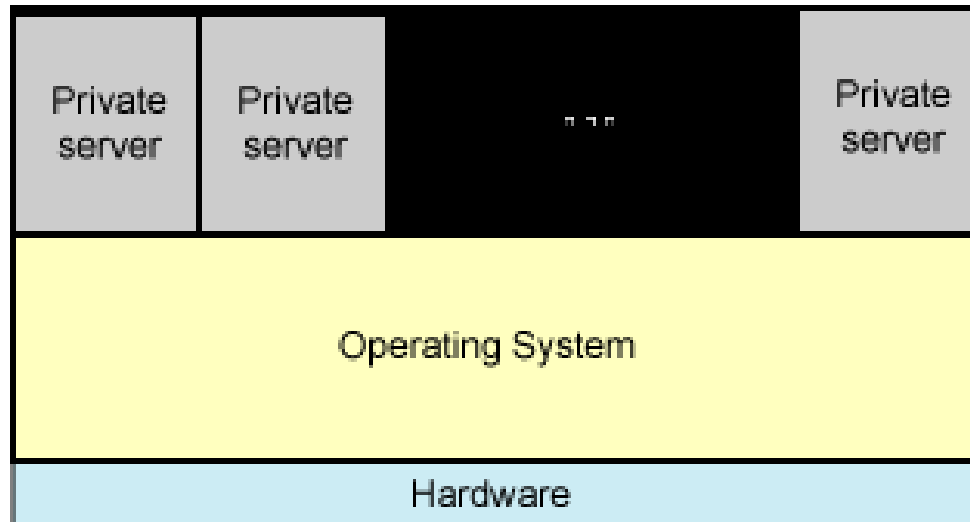
 execl("/bin/sh", "sh", "-i", (char *)0);
 die("exec sh");

 exit(0);
}

```

# FreeBSD Jail

- Where chroot jail was weak partitioning, FreeBSD jail is strong partitioning
  - Create virtual machines.
- Popularly used in ISPs.



# Freebsd jail

Stronger mechanism than simple chroot

**To run:**     **jail jail-path hostname IP-addr cmd**

- calls hardened chroot (no “../..” escape)
- can only bind to sockets with specified IP address and authorized ports
- can only communicate with processes inside jail
- root is limited, e.g. cannot load kernel modules



# Virtual OS on the Desktop

- VMWare, Parallels, KVM, Xen
- Different approaches
  - Hardware emulation
    - Emulation is where software is used to simulate hardware for a guest operating system to run in. This has been used in the past but is difficult to do and offers low performance.
  - Native virtualization (with hardware)
    - Native virtualization (or full virtualization) is where a type-2 hypervisor is used to partially allow access to the hardware and partially to simulate hardware in order to allow you to load a full operating system. This is used by emulation packages like VMware Server, Workstation, Virtual PC, and Virtual Server, Oracle Virtual Box
  - Paravirtualization
    - Paravirtualization is where the guest operating systems run on the hypervisor, allowing for higher performance and efficiency. For more technical information and videos on this topic, visit VMware's [Technology Preview for Transparent Virtualization](#). Examples of paravirtualization are Microsoft Hyper-V and VMware ESX Server.

# Problems with chroot and jail

## Coarse policies:

- All or nothing access to parts of file system
- Inappropriate for apps like a web browser
  - Needs read access to files outside jail  
(e.g. for sending attachments in Gmail)

## Does not prevent malicious apps from:

- Accessing network and messing with other machines
- Trying to crash host OS



# Isolation

---

## System Call Interposition

# System call interposition

Observation: to damage host system (e.g. persistent changes) app must make system calls:

- To delete/overwrite files: **unlink, open, write**
- To do network attacks: **socket, bind, connect, send**

Idea: monitor app's system calls and block unauthorized calls

## **Implementation options:**

- Completely kernel space (e.g. GSWTK) -- security extension architecture
- Completely user space (e.g. program shepherding)
- Hybrid (e.g. Systrace)

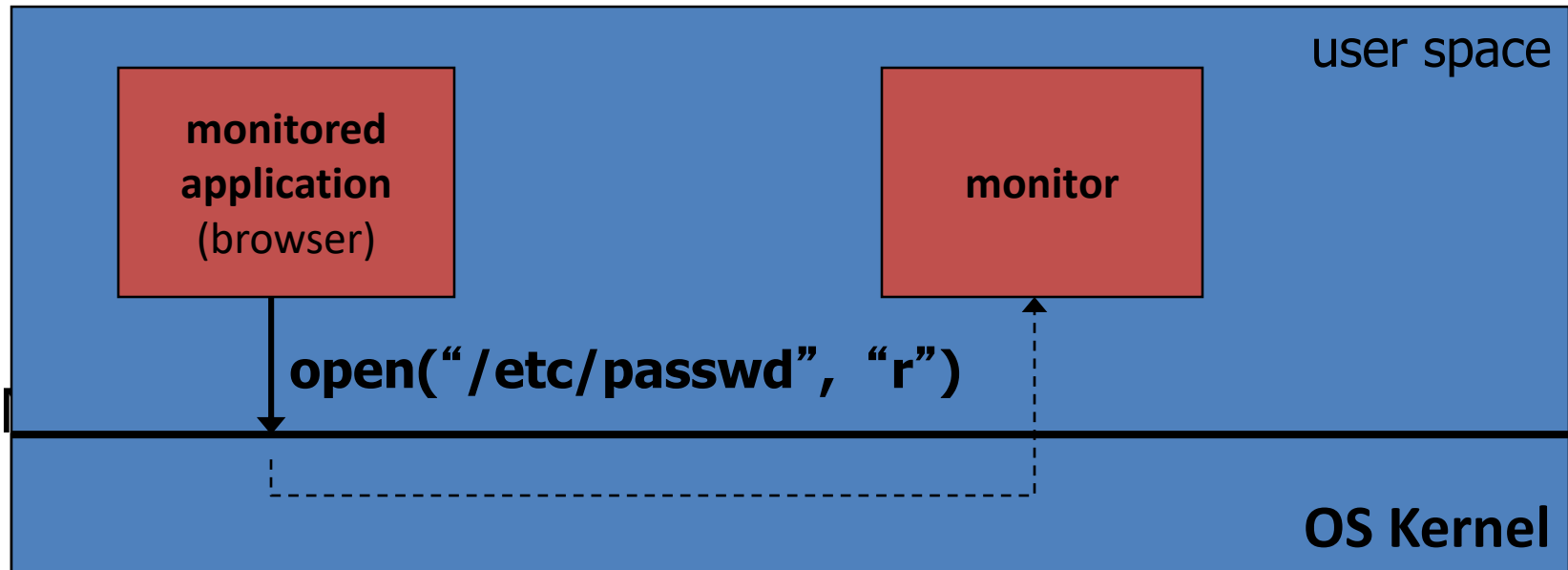
# Initial implementation (Janus)

[GWTB'96]

Linux **ptrace**: process tracing

process calls: **ptrace (... , pid\_t pid , ...)**

and wakes up when **pid** makes sys call.



# Complications

- If app forks, monitor must also fork
  - forked monitor monitors forked app
- If monitor crashes, app must be killed
- Monitor must maintain all OS state associated with app
  - current-working-dir (**CWD**), **UID**, **EUID**, **GID**
  - When app does “cd path” monitor must update its CWD
    - otherwise: relative path requests interpreted incorrectly

```
cd("/tmp")
open("passwd", "r")
```

```
cd("/etc")
open("passwd", "r")
```

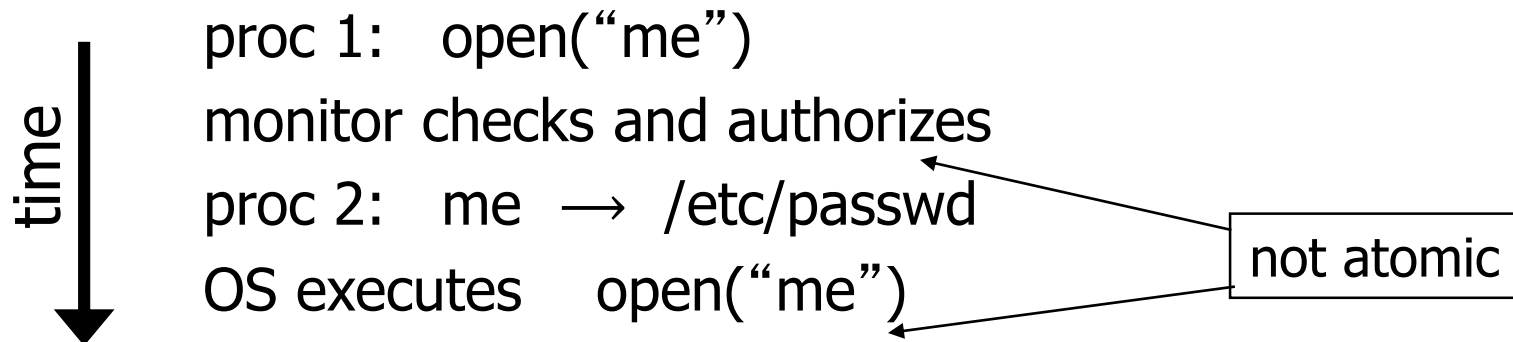
# Problems with ptrace

**Ptrace** is not well suited for this application:

- Trace all system calls or none
  - inefficient: no need to trace “close” system call
- Monitor cannot abort sys-call without killing app

Security problems: **race conditions**

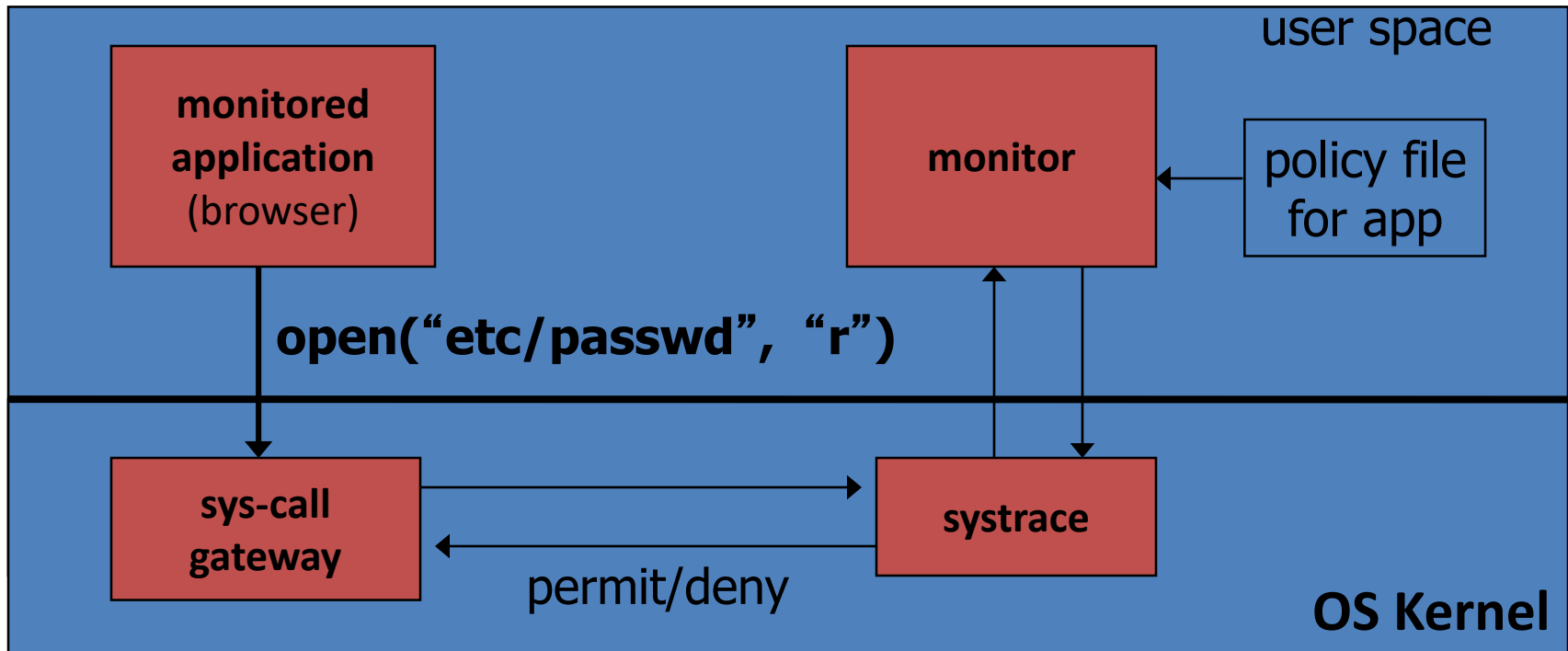
- Example: symlink: me → mydata.dat



Classic **TOCTOU bug**: time-of-check / time-of-use

# Alternate design: systrace

[P'02]



- systrace only forwards monitored sys-calls to monitor (efficiency)
- systrace resolves sym-links and replaces sys-call path arguments by full path to target
- When app calls **execve**, monitor loads new policy file



# Systrace Policies

Systrace executes the application without privileges and only elevates them to the desired level when required.

```
native-socket: sockdom eq "AF_INET" and socktype eq "SOCK_RAW" then permit as root
native-bind: sockaddr eq "inet-[0.0.0.0]:22" then permit as root
native-fsread: filename eq "/dev/kmem" then permit as :kmem
```

A simple policy for the *ls* binary. If *ls* attempts to list files in */etc*, Systrace disallows the access and */etc* does not seem to exist. Listing the contents of */tmp* works normally, but trying to *ls /var* generates a warning.

```
Policy: /bin/ls, Emulation: native
native-munmap: permit
[...] native-stat: permit
native-fsread: filename match "/usr/*" then permit
native-fsread: filename eq "/tmp" then permit
native-fsread: filename eq "/etc" then deny[enotdir]
native-fchdir: permit
native-fstat: permit native-fcntl: permit
[...] native-close: permit
native-write: permit
native-exit: permit
```

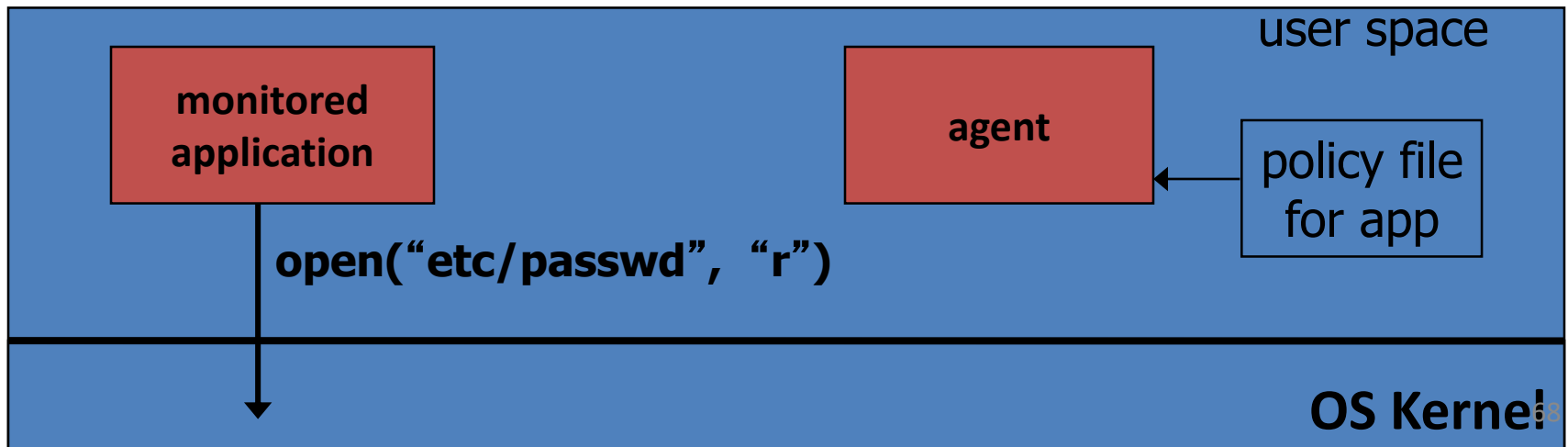
# Ostia: a delegation architecture

[GPR'04]

Previous designs use filtering:

- Filter examines sys-calls and decides whether to block
- Difficulty with syncing state between app and monitor (CWD, UID, ..)
  - Incorrect syncing results in security vulnerabilities (e.g. disallowed file opened)

A delegation architecture:



# Ostia: a delegation architecture

[GPR'04]

- Monitored app disallowed from making monitored sys calls
  - Minimal kernel change ( ... but app can call **close()** itself )
- Sys-call delegated to an agent that decides if call is allowed
  - Can be done without changing app  
(requires an emulation layer in monitored process)
- Incorrect state syncing will not result in policy violation
- What should agent do when app calls **execve**?
  - Process can make the call directly. Agent loads new policy file.

# Policy

Sample policy file:

```
path allow /tmp/*
path deny /etc/passwd
network deny all
```

Manually specifying policy for an app can be difficult:

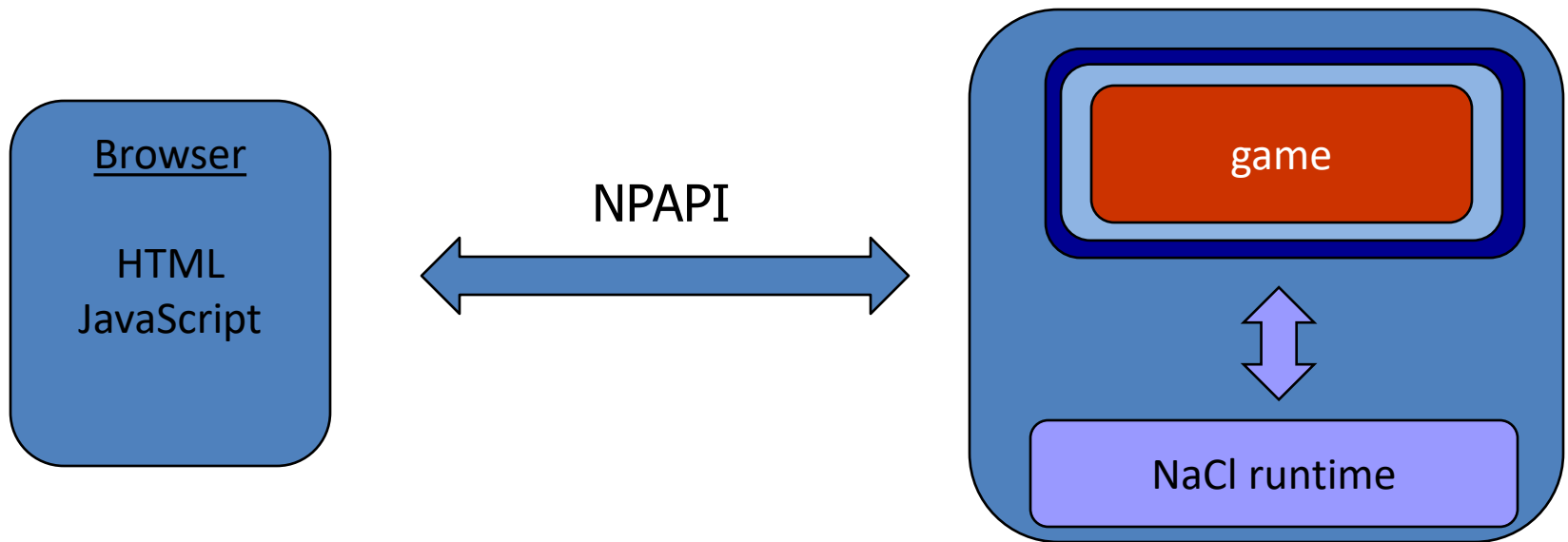
- Systrace can auto-generate policy by learning how app behaves on “good” inputs
- If policy does not cover a specific sys-call, ask user  
... but user has no way to decide

Difficulty with choosing policy for specific apps (e.g. browser) is the main reason this approach is not widely used

# Program Shepherding

| Restricting                | Least restrictive |                     | Most restrictive                                                    |                                                               |                                             |
|----------------------------|-------------------|---------------------|---------------------------------------------------------------------|---------------------------------------------------------------|---------------------------------------------|
| Code origins               | Any               |                     | Dynamically written code, if self-contained and no system calls     | Only code from disk, can be dynamically loaded                | Only code from disk, originally loaded      |
| Function returns           | Any               | Only to after calls | Direct call targeted by only one return                             | Random <code>xor</code> as in StackGhost [14]                 | Return only from called function            |
| Intra-segment call or jump | Any               |                     | Only to function entry points (if have symbol table)                |                                                               | Only to bindings given in an interface list |
| Inter-segment call or jump | Any               |                     | Only to export of target segment                                    | Only to import of source segment                              | Only to bindings given in an interface list |
| Indirect calls             | Any               |                     | Only to address stored in read-only memory                          | Only within user segment or from library                      | None                                        |
| <code>execve</code>        | Any               |                     | Static arguments                                                    | Only if the operation can be validated not to cause a problem | None                                        |
| <code>open</code>          | Any               |                     | Disallow writes to specific files (e.g., <code>/etc/passwd</code> ) | Only to a subregion of the file system                        | None                                        |

# NaCl: a modern day example



- game: untrusted x86 code
- Two sandboxes:
  - outer sandbox: restricts capabilities using system call interposition
  - Inner sandbox: uses x86 memory segmentation to isolate application memory among apps

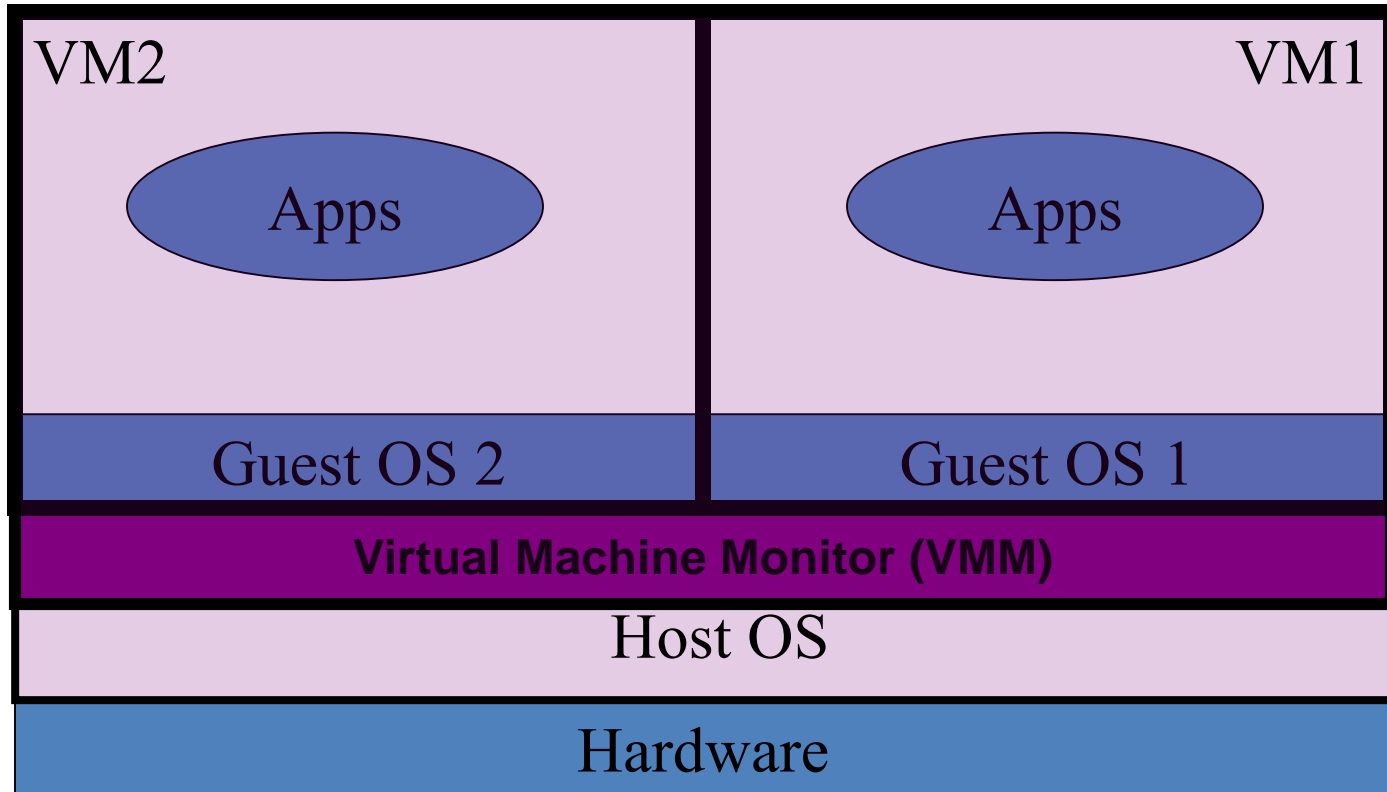


# Isolation

---

## Isolation via Virtual Machines

# Virtual Machines



Example: **NSA NetTop**

single HW platform used for both classified and unclassified data



# Why so popular now?

## **VMs in the 1960' s:**

- Few computers, lots of users
- VMs allow many users to shares a single computer

## **VMs 1970' s – 2000:** non-existent

## **VMs since 2000:**

- Too many computers, too few users
  - Print server, Mail server, Web server, File server, Database , ...
- Wasteful to run each service on different hardware
- More generally: VMs heavily used in cloud computing

# VMM security assumption

## **VMM Security assumption:**

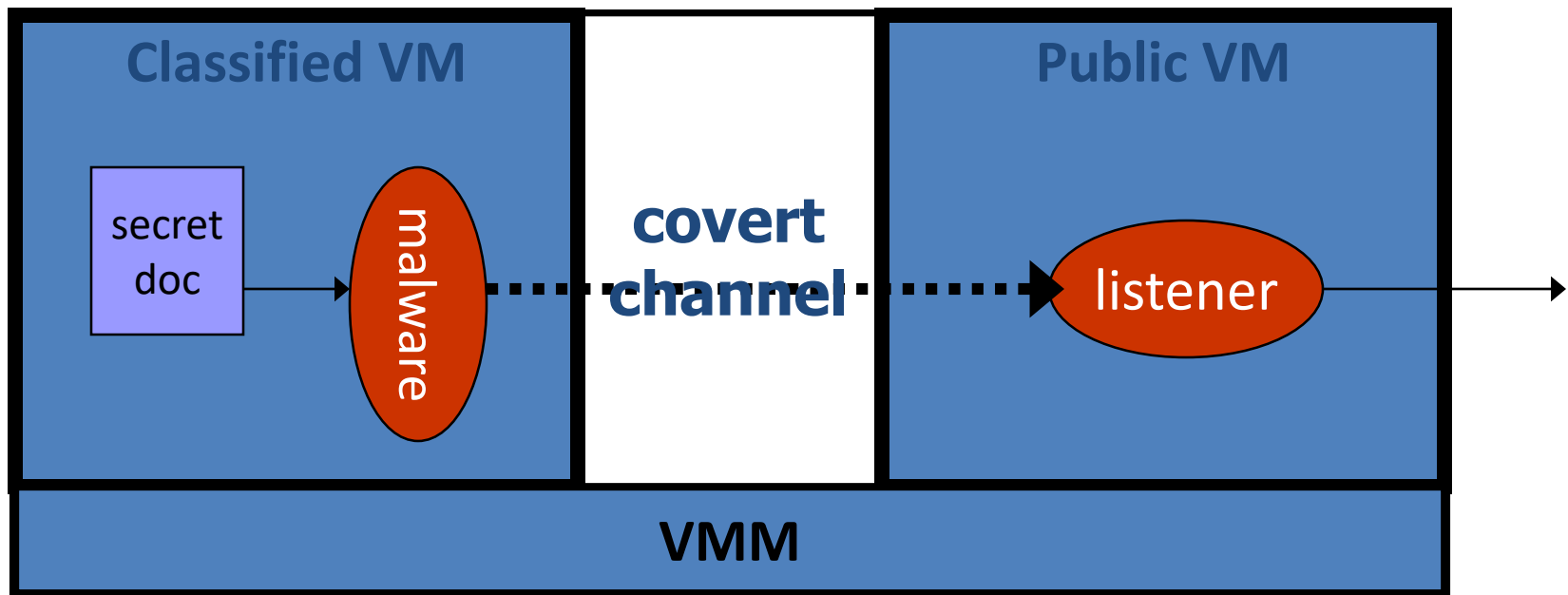
- Malware can infect guest OS and guest apps
- But malware cannot escape from the infected VM
  - Cannot infect host OS
  - Cannot infect other VMs on the same hardware

Requires that VMM protect itself and is not buggy

- VMM is much simpler than full OS
  - ... but device drivers run in Host OS

# Problem: covert channels

- **Covert channel:** unintended communication channel between isolated components
  - Can be used to leak classified data from secure component to public component



# An example covert channel

Both VMs use the same underlying hardware

To send a bit  $b \in \{0,1\}$  malware does:

- $b = 1$ : at 1:00am do CPU intensive calculation
- $b = 0$ : at 1:00am do nothing

At 1:00am listener does CPU intensive calc. and measures completion time

$$b = 1 \iff \text{completion-time} > \text{threshold}$$

Many covert channels exist in running system:

- File lock status, cache contents, interrupts, ...
- Difficult to eliminate all

Suppose the system in question has two CPUs: the classified VM runs on one and the public VM runs on the other.

Is there a covert channel between the VMs?

There are covert channels, for example, based on the time needed to read from main memory

# A Detour: Few Words about Rootkits

# Topics

## Rootkits

- User-mode Rootkits
- Kernel Rootkits
- Detecting Rootkits
- Recovery from a Rootkit

# What is a rootkit?

Collection of attacker tools installed after an intruder has gained access

- Log cleaners
- File/process/user hiding tools
- Network sniffers
- Backdoor programs



# Rootkit Goals

1. Remove evidence of original attack and activity that led to rootkit installation.
2. Hide future attacker activity (files, network connections, processes) and prevent it from being logged.
3. Enable future access to system by attacker.
4. Install tools to widen scope of penetration.
5. Secure system so other attackers can't take control of system from original attacker.

# Concealment Techniques

- Remove log and audit file entries.
- Modify system programs to hide attacker files, network connections, and processes.
- Modify logging system to not log attacker activities.
- Modify OS kernel system calls to hide attacker activities.

# Installation Concealment

- Use a subdirectory of a busy system directory like /dev, /etc, /lib, or /usr/lib
- Use dot files, which aren't in ls output.
- Use spaces to make filenames look like expected dot files: “. ” and “.. ”
- Use filenames that system might use
  - /dev/hdd (if no 4<sup>th</sup> IDE disk exists)
  - /usr/lib/libX.a (libX11 is real Sun X-Windows)
- Delete rootkit install directory once installation is complete.

# Attack Tools

- Network sniffer
  - Including password grabber utility
- Password cracker
- Vulnerability scanners
- Autorooter
  - Automatically applies exploits to host ranges
- DDOS tools

# History of Rootkits

**1989:** Phrack 25 Black Tie Affair: wtmp wiping.

**1994:** Advisory CA-1994-01 about SunOS rootkits.

**1996:** Linux Rootkits (lrk3 released.)

**1997:** Phrack 51 halflife article: LKM-based rootkits

**1998:** Silvio Cesare's kernel patching via kmem.

**1999:** Greg Hoglund's NT kernel rootkit paper

# History of Rootkits

**2005:** Sony ships CDs with rootkits that hide DRM and spyware that auto-installs when CD played.

**2006:** SubVirt rootkit moves real OS to a VM.

# Rootkit Types

## User-mode Rootkits

- **Binary Rootkits** replace user programs.
  - Trojans: ls, netstat, ps
  - Trojan backdoors: login, sshd.
- **Library Rootkits** replace system libraries.
  - Intercept lib calls to hide activities and add backdoors.

## Kernel Rootkits

- Modify system calls/structures that all user-mode programs rely on to list users, processes, and sockets.
- Add backdoors to kernel itself.

# Binary Rootkits

- Install trojan-horse versions of common system commands, such as ls, netstat, and ps to hide attacker activities..
- Install programs to edit attacker activity from log and accounting files.
- Install trojan-horse variants of common programs like login, passwd, and sshd to allow attacker continued access to system.
- Install network sniffers.



# Linux Root Kit (LRK) v4 Features

|            |                                               |
|------------|-----------------------------------------------|
| chsh       | Trojaned! User->r00t                          |
| crontab    | Trojaned! Hidden Crontab Entries              |
| du         | Trojaned! Hide files                          |
| fix        | File fixer!                                   |
| ifconfig   | Trojaned! Hide sniffing                       |
| inetd      | Trojaned! Remote access                       |
| linsniffer | Packet sniffer!                               |
| login      | Trojaned! Remote access                       |
| ls         | Trojaned! Hide files                          |
| netstat    | Trojaned! Hide connections                    |
| passwd     | Trojaned! User->r00t                          |
| ps         | Trojaned! Hide processes                      |
| rshd       | Trojaned! Remote access                       |
| sniffchk   | Program to check if sniffer is up and running |
| syslogd    | Trojaned! Hide logs                           |
| tcpd       | Trojaned! Hide connections, avoid denies      |
| top        | Trojaned! Hide processes                      |
| wted       | wtmp/utmp editor!                             |
| z2         | Zap2 utmp/wtmp/lastlog eraser!                |

# Linux Root Kit (LRK) v4 Trojans

ifconfig – Doesn't display PROMISC flag when sniffing.

login – Allows login to any account with the rootkit password.  
If root login is refused on your terminal login as "rewt".  
Disables history logging when backdoor is used.

ls – Hides files listed in /dev/ptyr. All files shown with 'ls -/' if SHOWFLAG enabled.

passwd – Enter your rootkit password instead of old password to become root.

ps – Hides processes listed in /dev/ptyp.

rshd – Execute remote commands as root: rsh -l  
rootkitpassword host command

syslogd – Removes log entries matching strings listed in /dev/ptys.

# Binary Rootkit Detection

## Use non-trojaned programs

- ptree is generally uncompromised
- tar will archive hidden files, the list with -t
- lsof is also generally safe
- Use known good tools from CD-ROM.

## File integrity checks

- tripwire, AIDE, Osiris
- rpm -V -a
- Must have known valid version of database offline or attacker may modify file signatures to match Trojans.

# Library Rootkits

- t0rn rootkit uses special system library libproc.a to intercept process information requested by user utilities.
- Modify libc
  - Intercept system call data returning from kernel, stripping out evidence of attacker activities.
  - Alternately, ensure that rootkit library providing system calls is called instead of libc by placing it in /etc/ld.so.preload

# Kernel Rootkits

Kernel runs in supervisor processor mode

- Complete control over machine.

Rootkits modify kernel system calls

- `execve` modified to run Trojan horse binary for some programs, while other system calls used by integrity checkers read original binary file.
- `setuid` modified to give root to a certain user.

Advantage—Stealth

- Runtime integrity checkers cannot see rootkit changes.
- All programs impacted by kernel Trojan horse.
- Open backdoors/sniff network without running processes.

# Types of Kernel Rootkits

## Loadable Kernel Modules

- Device drivers are LKMs.
- Can be defeated by disabling LKMs.
- ex: Adore, Knark

## Alter running kernel in memory.

- Modify /dev/kmem directly.
- ex: SucKit

## Alter kernel on disk.

# Kernel Rootkit Detection

List kernel modules

- lsmod
- cat /proc/modules

Examine kernel symbols (/proc/kallsyms)

- Module name listed in [] after symbol name.

# Kernel Rootkit Detection

Check system call addresses

- Compare running kernel syscall addresses with those listed in System.map generated at kernel compile.

All of these signatures can be hidden/forged.



# Knark

- Linux-based LKM rootkit
- Features
  - Hide/unhide files or directories
  - Hide TCP or UDP connections
  - Execution redirection
  - Unauthenticated privilege escalation
  - Utility to change UID/GID of a running process.
  - Unauthenticated, privileged remote execution daemon.
  - Kill -31 to hide a running process.
- modhide: assistant LKM that hides Knark from module listing attempts.

# Rootkit Detection

## Offline system examination

- Mount and examine disk using another OS kernel+image.
- Knoppix: live CD linux distribution.

## Computer Forensics

- Examine disk below filesystem level.
- Helix: live CD linux forensics tool.

# Rootkit Detection Utilities

## chkrootkit

- Detects >50 rootkits on multiple UNIX types.
- Checks commonly trojaned binaries.
- Examines log files for modifications.
- Checks for LKM rootkits.
- Use `-p` option to use known safe binaries from CDROM.

## carbonite

- LKM that searches for rootkits in kernel.
- Generates and searches frozen image kernel process structures.

# Detection Countermeasures

- Hide rootkit in unused sectors or in unused fragments of used sectors.
- Install rootkit into flash memory like PC BIOS, ensuring that rootkit persists even after disk formatting and OS re-installation.

# Rootkit Recovery

- Restore compromised programs from backup
  - Lose evidence of intrusion.
  - Did you find all the trojans?
- Backup system, then restore from tape
  - Save image of hard disk for investigation.
  - Restore known safe image to be sure that all trojans have been eliminated.
  - Patch system to repair exploited vulnerability.

# Key Points

- Backdoors allow intruder into system without using exploit again.
- Rootkits automatically deeply compromise a system once root access is attained.
- Rootkits are easy to use, difficult to detect.
- Don't trust anything on a compromised system—access disk from a known safe system, like a Knoppix CD.
- Recovery requires a full re-installation of the OS and restoration of files from a known good backup.

# References

1. Oktay Altunergil, "Scanning for Rootkits," <http://www.linuxdevcenter.com/pub/a/linux/2002/02/07/rootkits.html>, 2002.
2. Silvio Cesare, "Runtime kernel kmem patching," <http://vx.netlux.org/lib/vsc07.html>, 1998.
3. William Cheswick, Steven Bellovin, and Avriel Rubin, *Firewalls and Internet Security*, 2<sup>nd</sup> edition, 2003.
4. Anton Chuvakin, "An Overview of UNIX Rootkits," iDEFENSE whitepaper, 2003.
5. Dave Dittrich, "Rootkits FAQ," <http://staff.washington.edu/dittrich/misc/faqs/rootkits.faq>, 2002.
6. Greg Hoglund and Gary McGraw, *Exploiting Software: How to Break Code*, Addison-Wesley, 2004.
7. Samuel T. King et. al., "SubVirt: Implementing malware with virtual machines", <http://www.eecs.umich.edu/virtual/papers/king06.pdf>, 2006.
8. McClure, Stuart, Scambray, Joel, Kurtz, George, *Hacking Exposed*, 3<sup>rd</sup> edition, McGraw-Hill, 2001.
9. Peikari, Cyrus and Chuvakin, Anton, *Security Warrior*, O'Reilly & Associates, 2003.
10. pragmatic, (nearly) Complete Loadable Linux Kernel Modules, [http://www.thc.org/papers/LKM\\_HACKING.html](http://www.thc.org/papers/LKM_HACKING.html), 1999.
11. Marc Russinovich, "Sony, Rootkits and Digital Rights Management Gone Too Far," <http://blogs.technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx>
12. Jennifer Rutkowska, "Red Pill: or how to detect VMM using (almost) one CPU instruction," <http://www.invisiblethings.org/papers/redpill.html>, 2004.
13. Ed Skoudis, *Counter Hack Reloaded*, Prentice Hall, 2006.
14. Ed Skoudis and Lenny Zeltser, *Malware: Fighting Malicious Code*, Prentice Hall, 2003.
15. Ranier Wichman, "Linux Kernel Rootkits," <http://la-samhna.de/library/rootkits/index.html>, 2002.

# Intrusion Detection Systems (IDS)

Another Digression



# Intrusion and Intrusion Detection

- Intrusion : Attempting to break into or misuse your system.
- Intruders may be from outside the network or legitimate users of the network.
- Intrusion can be a physical, system or remote intrusion.

# Different ways to intrude

- Buffer overflows
- Unexpected combinations
- Unhandled input
- Race conditions

# Intrusion Detection Systems (IDS)

Signature Based:

Intrusion Detection Systems look for attack signatures, which are specific patterns that usually indicate malicious or suspicious intent.

Anomaly Detection Based:

Machine learning techniques used to characterize normal behavior from anomalous behavior

# Intrusion Detection Systems (IDS)

- Different ways of classifying an IDS

IDS based on

- anomaly detection
- signature based misuse
- host based
- network based

# Anomaly based IDS

- This IDS models the normal usage of the network as a noise characterization.
- Anything distinct from the noise is assumed to be an intrusion activity.
  - E.g flooding a host with lots of packet.
- The primary strength is its ability to recognize novel attacks.

# Drawbacks of Anomaly detection IDS

- Assumes that intrusions will be accompanied by manifestations that are sufficiently unusual so as to permit detection.
- These generate many false alarms and hence compromise the effectiveness of the IDS.

# Signature based IDS

- This IDS possess an attacked description that can be matched to sensed attack manifestations.
- The question of what information is relevant to an IDS depends upon what it is trying to detect.
  - E.g DNS, FTP etc.

# Signature based IDS (contd.)

- ID system is programmed to interpret a certain series of packets, or a certain piece of data contained in those packets, as an attack. For example, an IDS that watches web servers might be programmed to look for the string “phf” as an indicator of a CGI program attack.
- Most signature analysis systems are based off of simple pattern matching algorithms. In most cases, the IDS simply looks for a sub string within a stream of data carried by network packets. When it finds this sub string (for example, the “phf” in “GET /cgi-bin/phf?”), it identifies those network packets as vehicles of an attack.



# Drawbacks of Signature based IDS

- They are unable to detect novel attacks.
- Suffer from false alarms
- Have to be programmed again for every new pattern to be detected.

# Host/Applications based IDS

- The host operating system or the application logs in the audit information.
- These audit information includes events like the use of identification and authentication mechanisms (logins etc.) , file opens and program executions, admin activities etc.
- This audit is then analyzed to detect trails of intrusion.

# Drawbacks of the host based IDS

- The kind of information needed to be logged in is a matter of experience.
- Unselective logging of messages may greatly increase the audit and analysis burdens.
- Selective logging runs the risk that attack manifestations could be missed.

# Strengths of the host based IDS

- Attack verification
- System specific activity
- Encrypted and switch environments
- Monitoring key components
- Near Real-Time detection and response.
- No additional hardware

# Stack based IDS

- They are integrated closely with the TCP/IP stack, allowing packets to be watched as they traverse their way up the OSI layers.
- This allows the IDS to pull the packets from the stack before the OS or the application have a chance to process the packets.

# Network based IDS

- This IDS looks for attack signatures in network traffic via a promiscuous interface.
- A filter is usually applied to determine which traffic will be discarded or passed on to an attack recognition module. This helps to filter out known un-malicious traffic.

# Strengths of Network based IDS

- Cost of ownership reduced
- Packet analysis
- Real time detection and response
- Malicious intent detection
- Operating system independence

# Commercial ID Systems

- ISS – Real Secure from Internet Security Systems:
  - Real time IDS.
  - Contains both host and network based IDS.
- Tripwire – File integrity assessment tool.
- Bro and Snort – open source public-domain system.



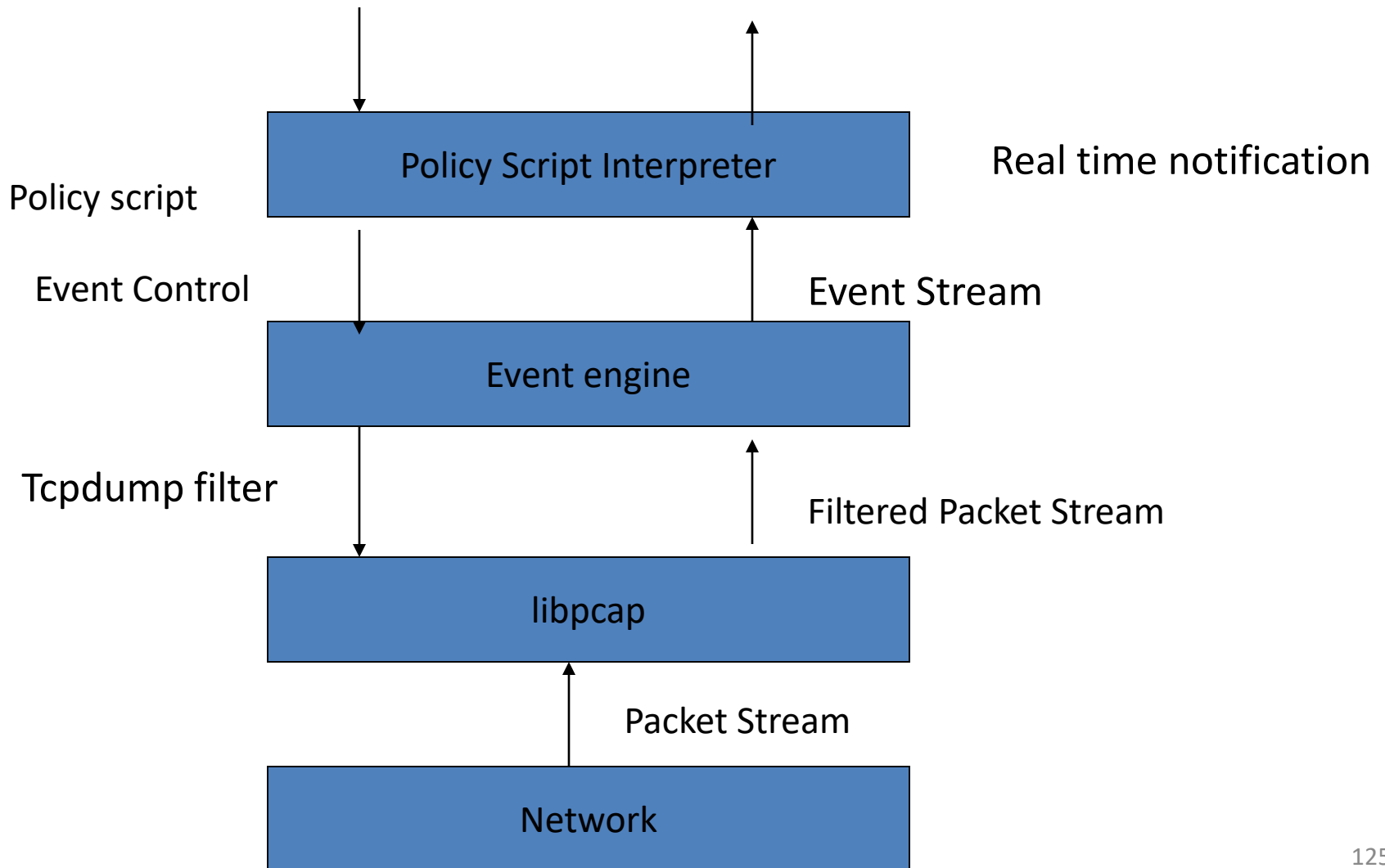
# Bro: Real time IDS

- Network based IDS
- Currently developed for six Internet applications: FTP, Finger, Portmapper, Ident, Telnet and Rlogin.

# Design goals for Bro

- High-speed, large volume monitoring
- No packet filter drops
- Real time notification
- Mechanism separate from policy
- Extensible

# Structure of the Bro System



# Bro - libpcap

- It's the packet capture library used by tcpdump.
- Isolates Bro from details of the network link technology.
- Filters the incoming packet stream from the network to extract the required packets.
- E.g port finger, port ftp, tcp port 113 (Ident), port telnet, port login, port 111 (Portmapper).
- Can also capture packets with the SYN, FIN, or RST Control bits set.

# Bro – Event Engine

- The filtered packet stream from the libpcap is handed over to the Event Engine.
- Performs several integrity checks to assure that the packet headers are well formed.
- It looks up the connection state associated with the tuple of the two IP addresses and the two TCP or UDP port numbers.
- It then dispatches the packet to a handler for the corresponding connection.

# Bro – TCP Handler

- For each TCP packet, the connection handler verifies that the entire TCP Header is present and validates the TCP checksum.
- If successful, it then tests whether the TCP header includes any of the SYN/FIN/RST control flags and adjusts the connection's state accordingly.
- Different changes in the connection's state generate different events.

# Policy Script Interpreter

- The policy script interpreter receives the events generated by the Event Engine.
- It then executes scripts written in the Bro language which generates events like logging real-time notifications, recording data to disk or modifying internal state.
- Adding new functionality to Bro consists of adding a new protocol analyzer to the event engine and then writing new events handlers in the interpreter.

# Future of IDS

- To integrate the network and host based IDS for better detection.
- Developing IDS schemes for detecting novel attacks rather than individual instantiations.



# VMM Introspection: [GR' 03]

protecting the anti-virus system

# Intrusion Detection / Anti-virus

Runs as part of OS kernel and user space process

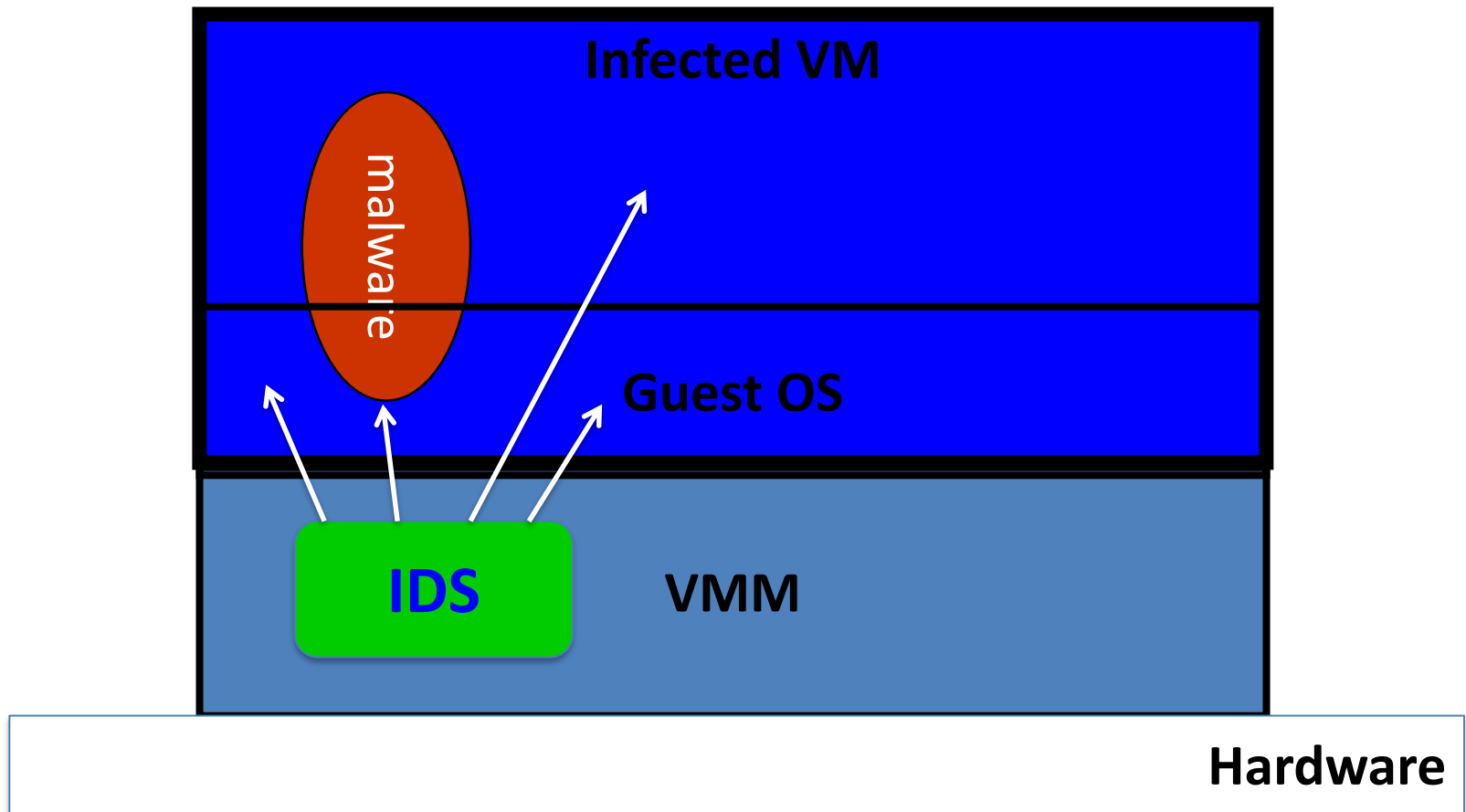
- Kernel root kit can shutdown protection system
- Common practice for modern malware

Standard solution: **run IDS system in the network**

- Problem: insufficient visibility into user's machine

Better: **run IDS as part of VMM (protected from malware)**

- VMM can monitor virtual hardware for anomalies
- VMI: Virtual Machine Introspection
  - Allows VMM to check Guest OS internals



# Sample checks

## **Stealth root-kit malware:**

- Creates processes that are invisible to “ps”
- Opens sockets that are invisible to “netstat”

### **1. Lie detector check**

- Goal: detect stealth malware that hides processes and network activity
- Method:
  - VMM lists processes running in GuestOS
  - VMM requests GuestOS to list processes (e.g. ps)
  - If mismatch: kill VM

# Sample checks

## 2. **Application code integrity detector**

- VMM computes hash of user app code running in VM
- Compare to whitelist of hashes
  - Kills VM if unknown program appears

## 3. **Ensure GuestOS kernel integrity**

- example: detect changes to `sys_call_table`

## 4. **Virus signature detector**

- Run virus signature detector on GuestOS memory



# Isolation

---

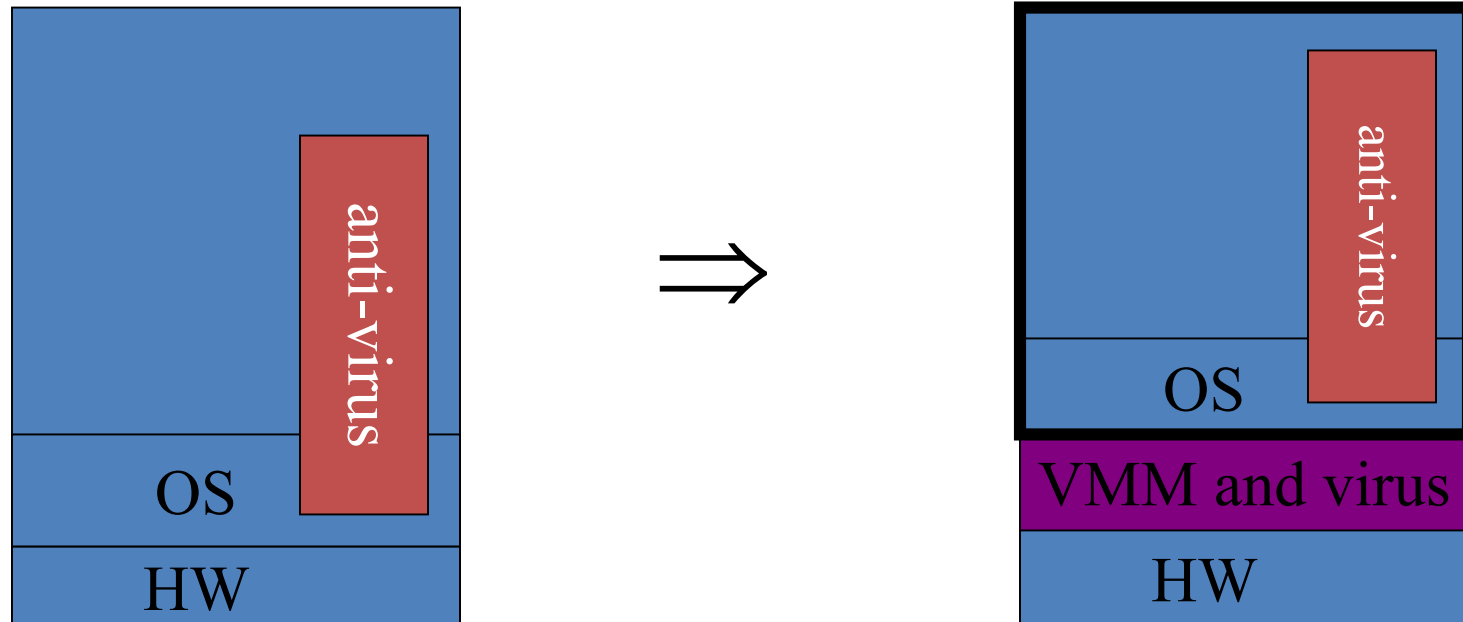
## Subverting VM Isolation

# Subvirt

[King et al. 2006]

Virus idea:

- Once on victim machine, install a malicious VMM
- Virus hides in VMM
- Invisible to virus detector running inside VM



# The MATRIX







# VM Based Malware (blue pill virus)

- **VMBR:** a virus that installs a malicious VMM (hypervisor)
- **Microsoft Security Bulletin: (Oct, 2006)**
  - Suggests disabling hardware virtualization features by default for client-side systems
- **But VMBRs are easy to defeat**
  - A guest OS can detect that it is running on top of VMM

# VMM Detection

Can an OS detect it is running on top of a VMM?

## Applications:

- Virus detector can detect VMBR
- Normal virus (non-VMBR) can detect VMM
  - refuse to run to avoid reverse engineering
- Software that binds to hardware (e.g. MS Windows) can refuse to run on top of VMM
- DRM systems may refuse to run on top of VMM

# VMM detection (red pill techniques)

- VM platforms often emulate simple hardware
  - VMWare emulates an ancient i440bx chipset
    - ... but report 8GB RAM, dual CPUs, etc.
- VMM introduces time latency variances
  - Memory cache behavior differs in presence of VMM
  - Results in relative time variations for any two operations
- VMM shares the TLB with GuestOS
  - GuestOS can detect reduced TLB size
- ... and many more methods [**GAWF' 07**]

# VMM Detection

Bottom line: **The perfect VMM does not exist**

VMMs today (e.g. VMWare) focus on:

Compatibility: ensure off the shelf software works

Performance: minimize virtualization overhead

- VMMs do not provide **transparency**
  - **Anomalies reveal existence of VMM**



# Isolation

---

## Software Fault Isolation

# Software Fault Isolation [Whabe et al., 1993]

**Goal:** confine apps running in same address space

- Codec code should not interfere with media player
- Device drivers should not corrupt kernel

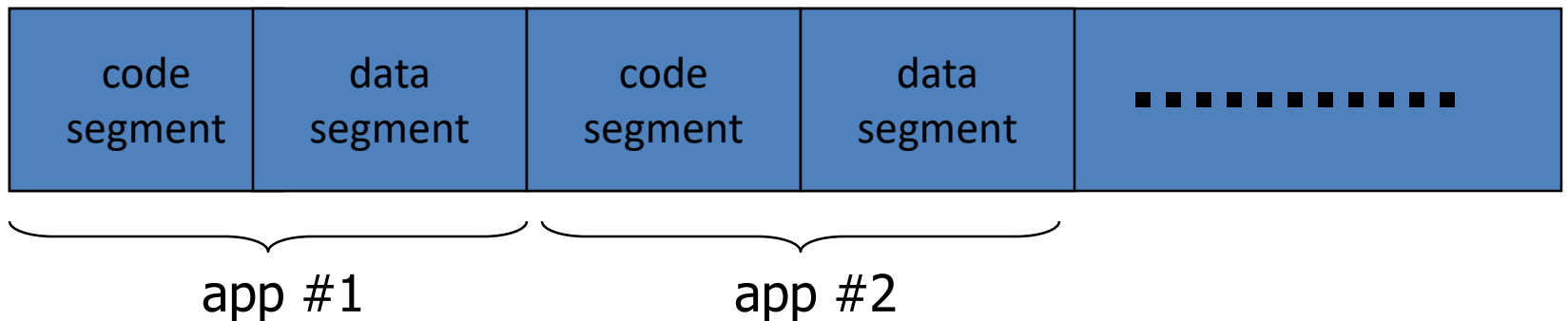
Simple solution: runs apps in separate address spaces

- Problem: slow if apps communicate frequently
  - requires context switch per message

# Software Fault Isolation

SFI approach:

- Partition process memory into segments



- Locate unsafe instructions: **jmp, load, store**
  - At compile time, add guards before unsafe instructions
  - When loading code, ensure all guards are present



# Segment matching technique

- Designed for M
- dr1, dr2:** de
  - compiler pretends that segments don't exist
  - **dr2** contains segment ID
- Indirect load instruction **R12 ← [R34]** becomes:

Guard ensures code does not  
load data from another segment

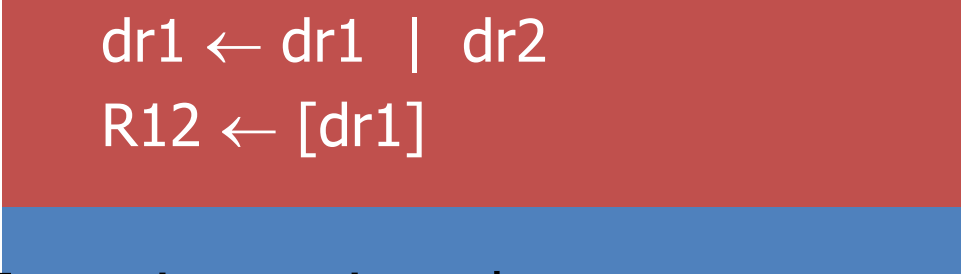
```
dr1 ← R34
scratch-reg ← (dr1 >> 20)
compare scratch-reg and dr2
trap if not equal
R12 ← [dr1]
```

```
: get segment ID
: validate seg. ID

: do load
```

# Address sandboxing technique

- **dr2:** holds segment ID
- Indirect load instruction **R12 ← [R34]** becomes:



dr1 ← dr1 | dr2  
R12 ← [dr1]

: zero out seg bits  
: set valid seg ID  
: do load

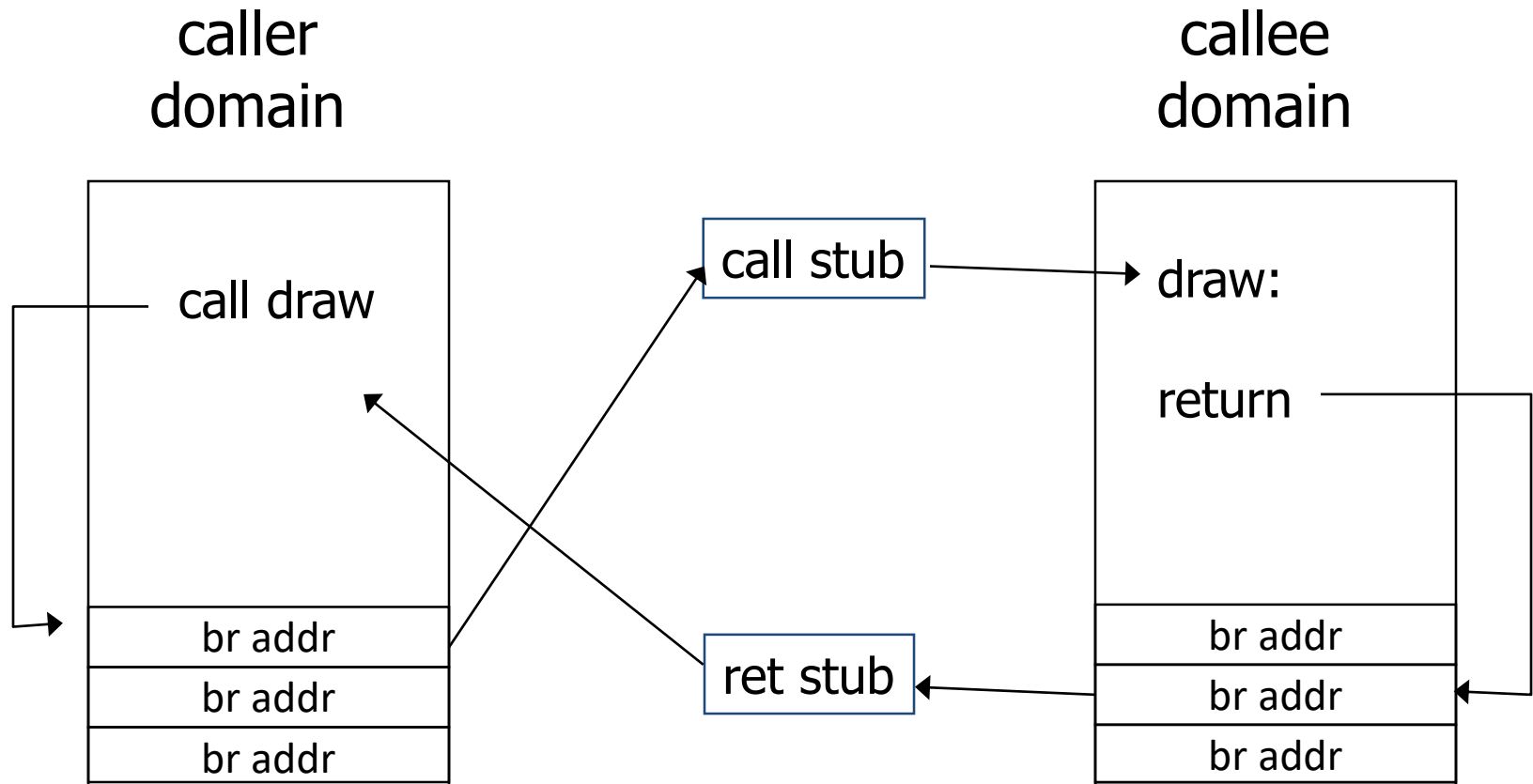
- Fewer instructions than segment matching  
... but does not catch offending instructions
- Similar guards places on all unsafe instructions

**Problem:** what if `jmp [addr]` jumps directly into indirect load?  
(bypassing guard)

**Solution:**

`jmp` guard must ensure `[addr]` does not bypass load guard

# Cross domain calls



- Only stubs allowed to make cross-domain jumps
- Jump table contains allowed exit points
  - Addresses are hard coded, read-only segment

# SFI Summary

- Shared memory: use virtual memory hardware
  - map same physical page to two segments in addr space
- Performance
  - Usually good: mpeg\_play, 4% slowdown
- Limitations of SFI: harder to implement on x86 :
  - variable length instructions: unclear where to put guards
  - few registers: can't dedicate three to SFI
  - many instructions affect memory: more guards needed

# Isolation: summary

- Many sandboxing techniques:  
*Physical air gap, Virtual air gap (VMMs),  
System call interposition, Software Fault isolation  
Application specific (e.g. Javascript in browser)*
- Often complete isolation is inappropriate
  - Apps need to communicate through regulated interfaces
- Hardest aspects of sandboxing:
  - Specifying policy: what can apps do and not do
  - Preventing covert channels