Lesson 7.5: Environmental Condition

SECURITY VULNERABILITIES IN C/C++ PROGRAMMING

Environmental Condition

Matt Bishop, Ph.D.
Professor of Computer Science,
UC Davis

UCDAVIS
Continuing and Professional Education

Slide 1: Defenses

Defenses

If the file system is trustworthy (as defined above), okay

Otherwise must ensure atomicity of “check” and “use” condition

- Be careful here! Systems implement functions in unexpected ways

Usual approach is “locking” a file

Slide 2: Linux Locks

Linux Locks

Advisory locking

- Useful between co-operating processes
- Process A locks file for shared (read) or exclusive (write) access; process B checks for lock before access

Mandatory locking

- Enforced for all processes
- Process A locks file; process B forced to honor lock

Slide 3: How to Do it

How to Do It

Advisory locks

- flock(2) system call
- fcntl(3) library call

Mandatory locks

- Requires file system be mounted with option mand
- Then relevant files have sgid bit set, group execute bit off (-1------0---)
- Use *fcntl* to lock, unlock
- Warning: applies to root, too!

Slide 4: Now…Don't Use Mandatory Locks

Now…Don't Use Mandatory Locks

Mandatory locks have problems

- Process 1 reads file; process 2 issues a mandatory lock for that file, alters it and unlocks it; then process 1 writes what it originally read
- root cannot override the lock; it must kill the process
- If write(2) overlaps with the lock, data may be modified after another process acquires the lock
- If read(2) overlaps with a write lock, it may read changes made after another process acquires the lock

Slide 5: Now… Don’t Use Mandatory Locks

Now…Don’t Use Mandatory Locks

Also, locking a file does not prevent the race condition

- You need to lock the directory

Slide 6: FreeBSD system calls

FreeBSD system calls

Openat(2) and friends

```
int openat(int fd, char *path, int flags)
```

Idea is that the directory is open, so inode information associated with next path element is obtained from open directory, so can't be switched

Note: be sure the directory you open is the rightmost one in the path that is untrusted