

CSE509 Spring 2007 Midterm Exam

Name: _____

- You may not use any reference materials during this exam.
- Electronic devices, including calculators, cell phones, mp3 players, and laptops are all prohibited.
- You may not use your own scratch paper. The exam has plenty and you can ask for more if needed.
- You may not leave the classroom once the exam has been distributed.
- Communicating with other students in any way is prohibited.

Academic Honesty: I understand that if I cheat on this exam in any way, I will receive the maximum possible penalty, including an F in this course.

Name (print):_____

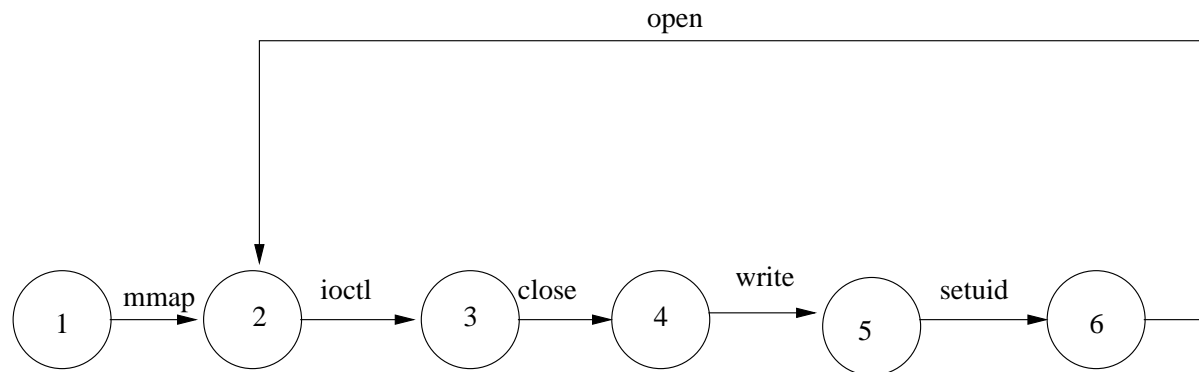
Signature:_____

CCured

(10 points) CCured was designed to prevent memory corruption via buffer overflows. Recall that it ensures that the program is type-safe at runtime, including that it cannot accidentally confuse an int and a pointer. Does CCured stop format-string attacks? Why or why not?

Mimicry Attacks

(10 points) Consider the following intrusion detection system model:



The program starts in state 1. You discover a buffer overflow that enables you to take control of the application when it is in state 6. After taking control of the application, your injected code can perform any sequence of system calls. Give a sequence of system calls, with arguments, that changes to user-id 0 and then writes to `/etc/shadow` without being detected by the intrusion detection system. Note that the IDS does not monitor arguments to system calls, so you can choose the arguments to the system calls as you see fit. The system calls take the following arguments:

```
void * mmap(void *start, int length, int prot , int flags, int fd, int offset);
int ioctl(int d, int request, ...);
int setuid(int uid);
int close(int fd);
int read(int fd, void *buf, int count);
int write(int fd, const void *buf, int count);
int open(const char *pathname, int flags);
```


I/O Data Oblivious IDS

(10 points) Consider a very powerful Intrusion Detection System that knows exactly the sequence of system calls the application will make, and knows all the arguments to those system calls, except the data the application writes to files and the network. So, for example, the IDS will know which files the application will open, but it doesn't know what the application will write to those files. Similarly, the IDS knows which network connections the application will make, but it doesn't know what data the application will transmit over those connections. List 5 security goals an attacker may still be able to violate while evading this powerful IDS. For example, an attacker could cause an e-commerce web server to send him the credit card numbers of other clients, because this would not require changing the system calls made by the web server, only the content of the data it sends to the attacker over the network.