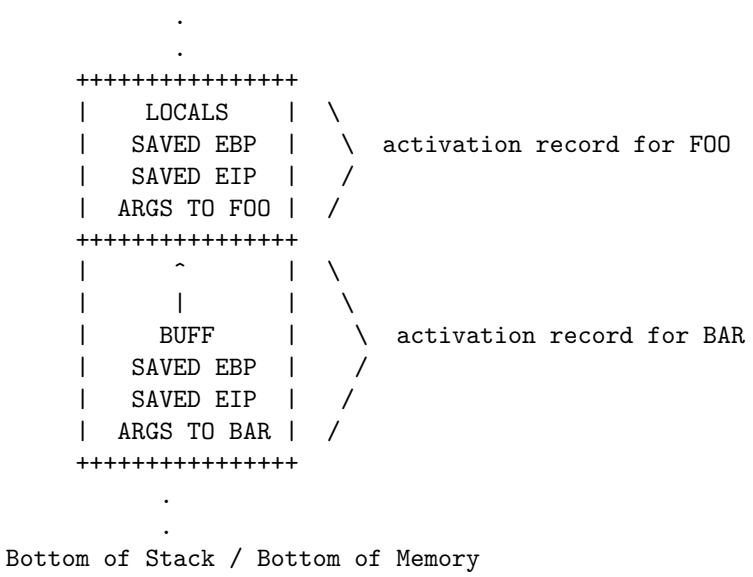
CS 155
Homework 1

Rafael Moreno Ferrer
SUID#: 05490330

Problem 1. *(Control Hijacking)*

a) In x86 the stack grows downwards. Explain how a stack-based overflow attack would work if the stack grew upwards instead.

For upward growing stacks overflowing an insecure buffer in the current activation record[1] will not generally result in a stack smashing attack since, at most, we will overwrite local variables but not any of the control data embedded in the stack (like saved eips, ebps or arguments). **However, stack smashing attacks can be done in this architecture by overflowing a buffer in a previous activation record.**



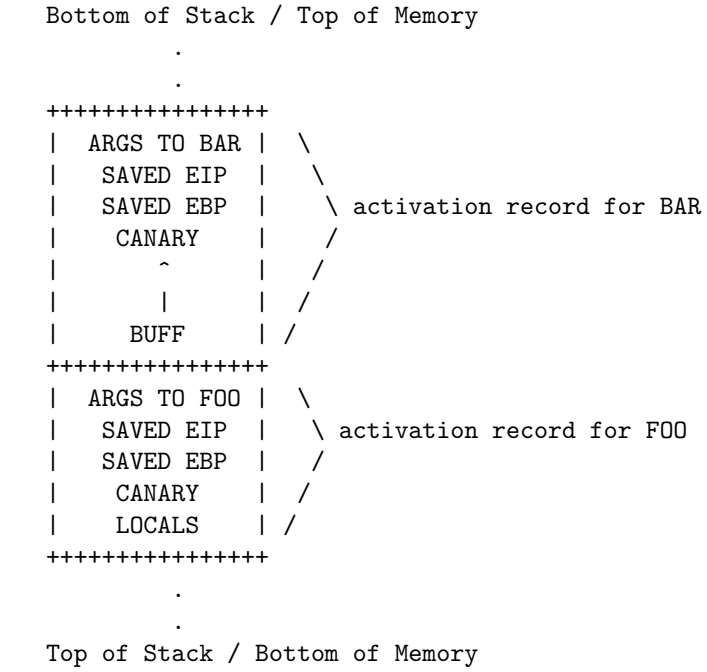
Suppose function BAR calls function FOO and function BAR has a local buffer BUFF. Inside function FOO there is code that copies data into BUFF unsafely. BUFF then can be overflown to overwrite the SAVED EIP for FOO and hijack control when FOO returns.

b) How would you implement StackGuard in an architecture where the stack grows upwards? What would be different from StackGuard on the x86?

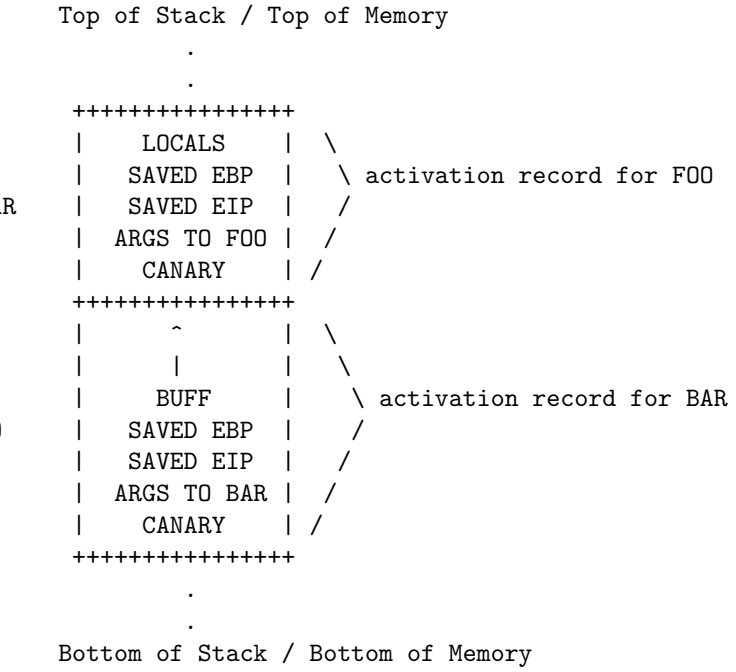
From the picture above we see that in order to overflow BUFF and overwrite the SAVED EIP for FOO we need to stomp first over ARGS TO FOO and then its SAVED EIP. To implement StackGuard in the upward growing architecture we can make the compiler **place a canary in the stack right before the arguments for a function call to the stack. Prior to function return we will verify the integrity of the current activation record by checking the canary** and kill the process if we detect corruption. This differs from x86 in fact that the canary in x86 has to defend against a buffer overflow in an activation record overwriting the saved eip of that activation record as opposed to a buffer overflow in previous activation record corrupting the saved eip of a subsequent activation record. Thus the placement of the canary has to be different. The following diagram shows the different placements.

[1] the activation record of the function being current ly executed

a) StackGuard layout for downward growing stack



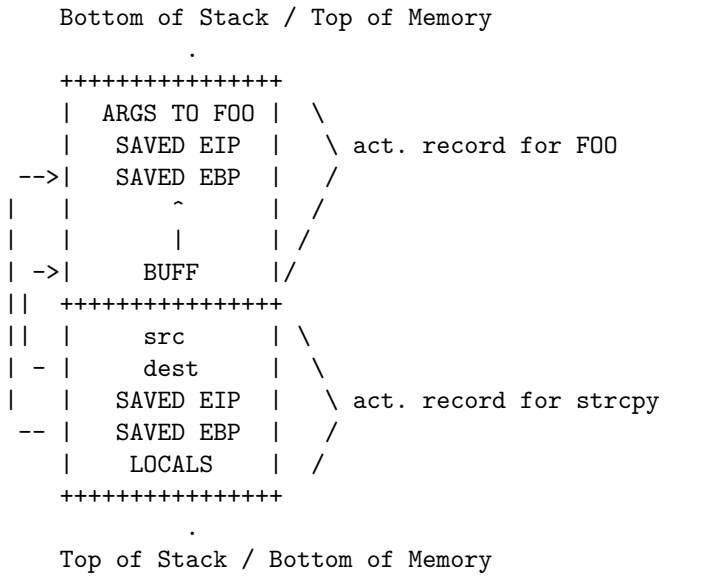
b) StackGuard layout for upward growing stack



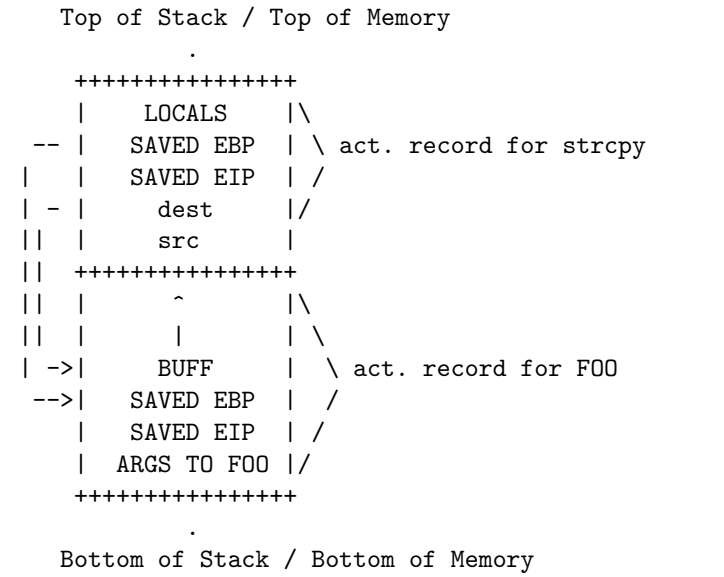
c) How would you implement LibSafe in an architecture where the stack grows upwards? What would be different from LibSafe on the x86?

The following diagram illustrates the stack layout for a call to strcpy from a function FOO in downward and upward growing stack architectures:

c) Libsafe layout for downward growing stack



d) Libsafe layout for upward growing stack



As discussed in lecture, in x86 Libsafe intercepts the call to `strcpy(dest, src)` and validates that there is sufficient space in the current stack frame via the test: `|SAVED EBP for strcpy - dest| > strlen(src)`. The picture clearly shows that **in the upward growing stack architecture in order to ensure `strcpy` does not overwrite `src` we would need the test: `|&src - dest| > strlen(src)`.** This approach of checking that the size of the data to be copied is no longer than the size of the space between the first argument to the Libsafe function and the start of the buffer being written to generalizes to other functions like `memcpy, strncpy, memset`, etc.

Problem 2. *(Memory management)*

The iOS `_MALLOC(size_t size, int type, int flags)` function allocates size bytes on the heap. Internally blocks are represented as a length field followed by a data field:

```
struct _mhead {
  size_t  mlen;
  char    dat[0];  }
```

The mlen field is used by the free() function to determine how much space needs to be freed. In iOS 4.x the _MALLOC function was implemented as follows:

```
1   void * \_MALLOC(size_t size, int type, int flags)  {
2     struct _mhead  *hdr;
3     size_t memsize = sizeof (*hdr) + size;
4     hdr = (void *)kalloc(memsize);  // allocate memory
5     hdr->mlen = memsize;
6     return  (hdr->dat);
7   }
```

In iOS 5.x the following two lines were added after line 3:

```
int o = memsize < size ? 1 : 0;
if (o)  return (NULL);
```

a) Why were these lines added in iOS5.x? Briefly describe an attack that may be possible without these lines.

These lines were added to prevent integer overflow attacks/bugs. Let MAX be the maximum value representable by a `size_t`. Suppose `size` is equal to MAX. Since `size_t` is an unsigned type then `memsize` will overflow to be 3 (MAX + 1 wraps around to 0, ..., MAX + 4 = MAX + sizeof(*hdr) = memsize wraps around to 3).

Now consider a scenario where we have a user program that takes an input string, allocates space in the heap to hold the string and then copies it. Suppose the attacker provided an input string of size MAX. The user will then call `_MALLOC` with `size = MAX` and get back a pointer `ptr` somewhere in the heap. The user will think `ptr` was allocated enough space to hold the string while in reality it was allocated only 3 bytes. When the user copies the string to `ptr` it will overwrite a bunch of memory next to his 3 allocated bytes and possibly trash memory in use by the heap allocator. Since it has likely overwritten user data as well as memory management data used by the heap allocator then subsequent calls that free that overwritten data will likely crash the program. At the very least, this will be a denial of service attack.

If the attacker knows the state of memory in the user program (or has the ability to massage the heap to a known state) and hence knows what the memory next to his allocated 3 bytes looks like he can fabricate malicious input to overwrite the memory management data used by `free`. This can result in a control hijacking attack much like in the double free exploit from project 1.

b) In iOS the kernel heap is divided into zones. When the zone allocator is called it allocates a new zone in a random location in kernel space. What security purpose does randomization serve in this context?

Relating to the last point made in a) if the attacker knows the state of the heap in the user process or if he has the ability to massage it to a known state (as in heap feng shui), then he will be able to exploit bugs like the one described in a) to overwrite memory management data to hijack control. Randomization makes it very difficult for an attacker to exactly know the state of the heap or massage it to a known state since the state changes from one run to the next.

In summary, randomization helps in making less robust/more unreliable attacks where the attacker can know the state of the heap.

Problem 3. *(Sandboxing)*

For a) and b): in general, if we have an application whose functionality is tightly coupled with other applications (i.e. it needs to constantly establish many channels of communications with other applications to do its work) then system-call interposition would be preferred to VM-sandboxing. If an OS-level gap was established through VM-sandboxing then the application would need to be going through the VMM to establish network connections to processes in other VMs (TCP, UDP, ...), which have their own overhead and may turn out to be a prohibitive cost.

On the other hand if the application is not tightly coupled to other applications (e.g. a text editor) then VM-sandboxing would not be prohibitive and may be preferred for more security.

a) Explain in what settings would you use VM-based sandboxing rather than system call interposition.

As mentioned above, VM-sanboxing can be used in cases where the application is loosely coupled with other applications. Another scenario in which to prefer VM-sandboxing is the following: if we have an application for which it is hard to comprehend all the permissions it needs to operate correctly (for example Microsoft Exchange) then it might be nearly impossible to write a policy file to be used in system-call interposition. In this cases VM-sandboxing might be preferred.

b) Explain in what settings would you use system call interposition rather than VM-based sandboxing.

As explained above we might want to use system call interposition when the application in question is tightly coupled with other applications and needs to be constantly establishing many communication channels to other applications inside the same machine.

c) In class we discussed a covert channel between two VMs based on CPU utilization and a synchronized clock between the VMs. One might try to block this covert channel by preventing the VMs from synchronizing their clocks, e.g. by presenting each VM with a different time of day. You may assume the clocks run at normal speed, but are shifted by a random amount for each VM. Explain how an attacker can defeat this defense.

Let M be the VM where the malware resides and L be the VM where the listener resides. Suppose M's clock trails `offset` second behind L's clock (i.e. `time_of_day(L) = time_of_day(M) + offset`). Now consider the following algorithm for discovering `offset` / synchronizing the clocks:

```
Every day at 12:00am malware does CPU intensive computation

for i from 0 to NUM_SECONDS_IN_DAY - 1 {
  at 12:00am + i seconds listener does CPU intensive computation and measure completion time
  if completion_time > threshold:
    offset = i; break;
  else continue
}
```

After NUM_SECONDS_IN_DAY days the malware can assume that the listener has figured out the correct offset since the for loop executes at most NUM_SECONDS_IN_DAY times. Hence, on day NUM_SECONDS_IN_DAY + 1 transmission of protected data can start according to:

```
To send a bit b = {0, 1} malware does:
  if b = 1: at 12:00am + offset do CPU intensive calc
  if b = 0: at 12:00am + offset do nothing

At 12:00am listener does CPU intensive calc and measures completion time:
  b = 1 if and only if completion time > threshold
```

Of course, this scheme is only theoretical since it takes NUM_SECONDS_IN_DAY days (about 200 years) only for the synchronization phase. However, this can be fixed in the following way.

The fact that we wanted to synchronize the clocks to the same second of the day was arbitrary. We can synchronize them to the same second of the minute and still have an effective scheme, i.e. we want to figure out instead `offset = second_of_the_minute(L) - second_of_the_minute(M)` where for example `second_of_the_minute(12:00:59pm) = 59`. The scheme now becomes:

```
Every minute at 0 seconds malware does CPU intensive computation

for i from 0 to NUM_SECONDS_IN_MINUTE - 1 {
  at start_of_minute + i seconds listener does CPU intensive computation and measure completion time
  if completion_time > threshold:
    offset = i; break;
  else continue
}

After 60 minutes malware can assume listener knows the offset and start transmitting data at minute 61.

To send a bit b = {0, 1} malware does:
  if b = 1: at start_of_minute + offset do CPU intensive calc
  if b = 0: at start_of_minute + offset do nothing

At start_of_minute listener does CPU intensive calc and measures completion time:
  b = 1 if and only if completion time > threshold
```

Of course, if this is so fine grained that causes problems in synchronization one can move to a more coarse synchronization level like second of the hour and still get reasonable run time.

d) Suggest another method by which the covert channel based on CPU utilization can be blocked.

Three come to mind:
1. Time-slicing: Have all VMs be given an equal slice of time when scheduled in the CPU. In this way the completion time of the listener's computation will be unaffected by the intensity of the computation being done on the other VM by the malware, thus defeating the attack.
2. Separate resources: assign the VMs to run on different cores. As in the previous approach, the completion time of the listener's computation will be unaffected by the intensity of the computation being done in the VM where the malware resides.
3. Randomly introduce idle time when a process is scheduled into the CPU: this is the least efficient, but by introducing random delays some 0 bits sent by the malware will be corrupted to 1's making the covert channel dirty.

Problem 4. *(TOCTOU)*

Consider the following code snippet from `foo.c`:

```
1a.  if (!stat("./file.dat", buf)) return;   // Abort if file exists.
2a.  sleep(10);                              // Sleep for 10 seconds.
3a.  fp = fopen("./file.dat", "w" );
4a.  fprintf(fp, "Hello world" );
5a.  close(fp);
```

a) Suppose this code is running as a setuid root program. Give an example of how this code can lead to unexpected behavior that could cause a security problem. (try using symbolic links.)

Suppose there is a malicious program `bar.c` that simply does the following:

```
1b.  symlink ("/etc/passwd", "./file.dat");
```

i.e. it creates a symlink from `./file.dat` to `/etc/passwd` (assuming `./file.dat` does not exist). Suppose furthermore that the programs `foo` and `bar` are both running at the same time, with the same current working directory environment variable and that `foo` is running as a seteuid root program. Consider the following scenario: A file `./file.dat` does not exists when both programs start executing. `foo` is scheduled first and gets to line 1a. passes the test then goes on to line 2a. and gets switched out while sleeping. `bar` then gets scheduled in and executes line 1b successfully creating a symlink from `./file.dat` to `/etc/passwd` and exits. Then `foo` gets switched in again and continues to execute lines 3a through 5a. Since it has root EUID then `foo` will be allowed to open `/etc/passwd` and write "Hello world" to the beginning of the file.

This represents a security problem since the malicious program has achieved the password file to be overwritten, possibly corrupting the information for some user(s) and thus at least creating a denial of service attack against those user(s) since their credentials have been corrupted. Note: one can add a call to `remove("./file.dat");` before the `symlink` call in `bar` to make the attack work sometimes in cases where the file `./file.dat` existed prior to starting.

b) Suppose the sleep(10) is removed from the code above. Could the problem you identified in part (a) still occur? Please explain.

The problem in (a) can still occur, however it becomes less probable. The problem in (a) happened because `bar` got switched in while `foo` was sleeping. This was likely to occur since sleeping for 10 seconds will probably cause the scheduler to switch that process out and some other process in. By removing the `sleep` call we only decrease the probability of that exact interleaving, however it is still possible for `bar` to get switched in right before the call to `fopen` in `foo`, which would result in the same problem.

c) How would you fix the code to prevent the problem from part (a)?

The problem comes from the fact that checking in the file exists and opening it is not done atomically. According to the Linux man pages for open:

```
If O_CREAT and O_EXCL are set, open() shall fail if the file exists. The check for the existence of the
file and the creation of the file if it does not exist shall be atomic with respect to other threads
executing open() naming the same filename in the same directory with O_EXCL and O_CREAT set. If O_EXCL
and O_CREAT are set, and path names a symbolic link, open() shall fail and set errno to [EEXIST], regardless
of the contents of the symbolic link. If O_EXCL is set and O_CREAT is not set, the result is undefined.
```

Hence we can use the `O_EXCL, O_CREAT` files to make the existence checking and file opening atomic in the above code as follows:

```
1a.  int fp = open("./file.dat", O_CREAT | O_EXCL, 0644);
2a.  if (fp == -1) return;
4a.  fprintf(fp, "Hello world" );
5a.  close(fp);
```

Another way to prevent this problem is by using mandatory file locks in `foo.c`.

Problem 5. *(Soundness and completeness for static code analysis)*

a) A false alarm occurs when a tool reports an error, but the program the tool is analyzing does not contain an error. Can a tool that reports a false alarm be sound? Complete?

Completeness: By definition, a false alarm means reporting/flagging as an error something that is not an error in reality. A complete tool only reports things that are errors in reality. **Hence, a tool that report false alarms can definitely not be complete**.
Soundness: Soundness requires the program to report all real errors, plus possibly some false alarms. **Hence, a tool that reports false alarms can be sound if and only if it also reports all real errors.**

b) Suppose a company sets up an Android app marketplace for its employees. The company is going to use an analysis tool to check apps for security vulnerabilities before it promotes them to its employees. Which tool property is critical to the company for this purpose: soundness or completeness?

Argument for soundness: Consider a company that has a very high sensitivity to vulnerabilities (e.g. a governmental organization that stores highly classified national security information or intelligence, or a company that stores very sensitive consumer data such as health records, etc) and hence wants to be *absolutely certain* that the apps it promotes to its employees do not contain errors. Its sensitivity to vulnerabilities is so high that the company does not mind rejecting apps that did not actually contain errors and does not have resources or want to spend them investigating whether the apps it forbids are actually insecure. A sound tool will fit its purposes best since it will report all the real errors plus some false alarms. The company can just forbid all apps for which the tool reported errors. This would to ensure all apps it promotes to its employees are secure. **Alternatively,** if the company is willing to spend a lot of resources to be certain that the apps it promotes to its employees do not contain errors while accepting as many apps as possible the company will then have to devote resources to sift through the reports and discern between false alarms and real errors.

I believe there are arguments for both why you would want soundness or completeness in the tool and they both have tradeoffs. The decision whether to prefer one property over the other has to do with the tradeoff between *sensitivity to vulnerabilities* in the apps and *resources spent investigating* the vulnerabilities. Of course, another consideration is the quality of the tool (i.e. if we have the trivial sound tool that reports everything, or the trivial complete tool that reports nothing then these arguments don't matter) but we will not worry about that and assume the tool has "decent" quality. An argument for completeness is given as a footnote.[2]

c) Theoretically, suppose a tool is both sound and complete. When the tool is used to analyze the following code that may contain a vulnerability, what property of the loop determines whether the tool will report an error?

```
int main()
{
  int x = 0;
  while ( x < 10 ) { /* loop while x is less than 10 */
       ...  /* do some stuff that might change the value of x  */
  }
  ... /* do something insecure */;
}
```

(We assume the loop does not contain any insecure code)

Termination of the while loop (without exiting from main) on some possible path of execution: A sound and complete tool will report an error *if and only* if there is a vulnerability in the code. There is a vulnerability in the code if and only if the code after the while loop ever gets executed under some possible path of execution. This happens if and only if the loop terminates without exiting from main under some possible path of execution.

[2] **Argument for completeness:** Consider a company which does not want to spend many resources finding vulnerabilities and does not mind too much not covering all the possible vulnerabilities. A complete tool provides no false positives and only true positives (though not all of them). Hence a complete tool provides **actionable information** that the company can use right away to locate vulnerabilities in the apps its promoting to its employees. Even though the tool might fail to report some vulnerabilities it will give information that the company does not need to further validate and hence spend resources on. This is in contrast to a sound tool that may provide a lot of false alarms, leaving the company with no immediately actionable information and no clear sense of where to start looking. Thus a complete tool suits well a company with low sensitivity for vulnerabilities who is not looking to spend too much finding vulnerabilities.

Problem 6. *(Changing your Unix password)*

My answers assume the rules for `seteuid` described in `http://linux.die.net/man/2/seteuid`.

a) The password file is owned by the system (root) and readable by any user. Write appropriate permissions in the symbolic notation illustrated above. Any answer is acceptable for group permissions.

```
-rw-r--r--
```

b) The passwd program is owned by the system (root). What Unix feature allows an ordinary user to run passwd and change their password? Explain.

`seteuid`. It allows an unprivileged user to change his effective user id (the one used to evaluate permissions) to their SUID or their RUID. If a user process has SUID set to root then he can successfully call `seteuid(root)` to set EUID = root and then run the passwd program to change their password.

c) When a normal user, say "bob", runs passwd, passwd starts with:
Real-UID = bob
Effective-UID = bob
Saved-UID = root
The program makes a system call "seteuid(0)". What will be the Real-UID, Effective-UID, Saved-UID after this call?

Real-UID = bob
Effective-UID = root
Saved-UID = root

d) Suppose the program called "seteuid(alice)" instead, before calling "seteuid(0)". What would be the Real-UID, Effective-UID, Saved-UID after this call?

Real-UID = bob
Effective-UID = bob
Saved-UID = root

e) Suppose the program called "seteuid(alice)" after calling "seteuid(0)". What would be the Real-UID, Effective-UID, Saved-UID after this call?

Real-UID = bob
Effective-UID = alice
Saved-UID = root

f) Of course, passwd does not call "seteuid(alice)". Explain why passwd can write /etc/passwd and change password for user "bob" after the call seteuid(0).

After the call to seteuid(0) the effective user id of the password process is root (see c)). When trying to open the password file with write privileges the OS will check, according to the file permissions for /etc/passwd, if the process has permissions to write to the file. Since, by a), the only user id who can write to the file is root and the EUID of the process is root then this check will pass and the process will be allowed to open and write to the file.

g) Suppose passwd reads some other user input and does some other action after changing the password file. For example, we might want a custom version of passwd that writes into a log file owned by bob, when bob changes his password. What system call would you recommend after writing the password file and before doing other actions? What will be the Real-UID, Effective-UID, Saved-UID after the system call you recommend?

After writing to the password file do `seteuid(bob)` before doing any other actions. After this system call the RUID, EUID, and SUID will be

Real-UID = bob
Effective-UID = bob
Saved-UID = root