

Computer Science CS 4/53401 Secure Programming
Fall, 2014
Midterm
November 5, 2014

Please be brief; Irrelevant or incorrect material will cost you points.

1. (25 points) Can a security program be insecure? Why or why not?

Absolutely: for example, a program that checks passwords could have many vulnerabilities.

2. (25 points) Write code to read in and validate the name of a file in the current folder in a Linux/Unix computer.

Have to look here for:

- (a) The input statement should limit the number of characters read, or read into a dynamically allocated structure (like using `#include <string>` in C++) Thus any `cin.get` function is OK, provided it either reads only one character or includes a max of characters to read. At any rate,

```
cin >> a
```

where `a` is a character array is wrong and should cost points.

- (b) The program should then check that the input corresponds to a file name; it suffices if it checks that there are only alphanumerics `.,-` and a few other characters in the string. Mark points off if it checks for strange characters to disqualify the string; it should really only accept strings if it is of the form they expect, even if it rejects some perfectly valid inputs.

3. (25 points) How would you protect the confidentiality of data in a laptop that can be stolen?

One word: encrypt the data.

4. (25 points) Does the account you use on your machine have admin privileges? Why or why not?

They shouldn't. (It is OK if they say they do and why they should not). The reason for why they should not is that if they have too many privileges and something happens, too much damage is done. The "something happens" can be a mistake, a virus attack, or something else.