

EECE 412, Fall 2009

Quiz #4

This quiz consists of 6 pages. Please check that you have a complete copy. You may use both sides of each sheet if needed.

Your Family name: _____

Your Given name: _____

Your student ID: _____

#	Points	Out of
1		6
2		3
3		12
TOTAL		21

Name of your left neighbor: _____

Name of your right neighbor: _____

ATTENTION: When necessary, make reasonable assumptions and state them clearly in your solutions.

1. Consider the following example code in C.

```
void foo (int a, char* s) {
    char buffer[10];
    strcpy(buffer, s);
}
```

```
void main( int argc, char* argv[ ] ) {
    foo(1, argv[1]);
}
```

If everything goes fine when function foo is called, then the memory layout during execution of foo is shown in the following figure, where the thick black arrow shows how the program counter would change on the return from foo to main.

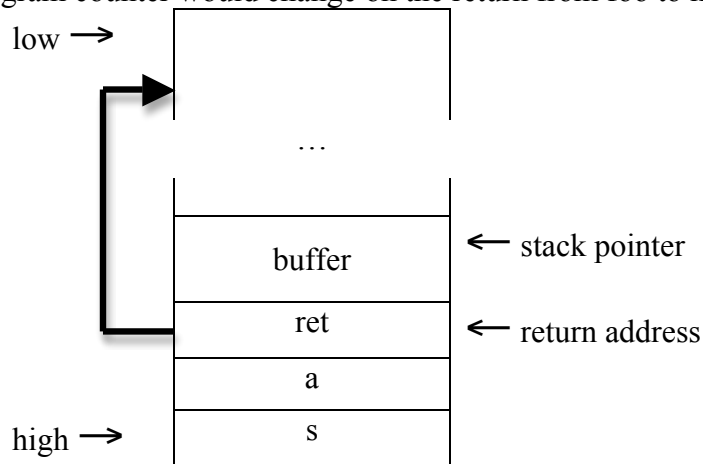


Figure 1.

Now, suppose a buffer overflow has occurred in foo, which resulted in the following memory layout. Such an overflow would generally crash the program.

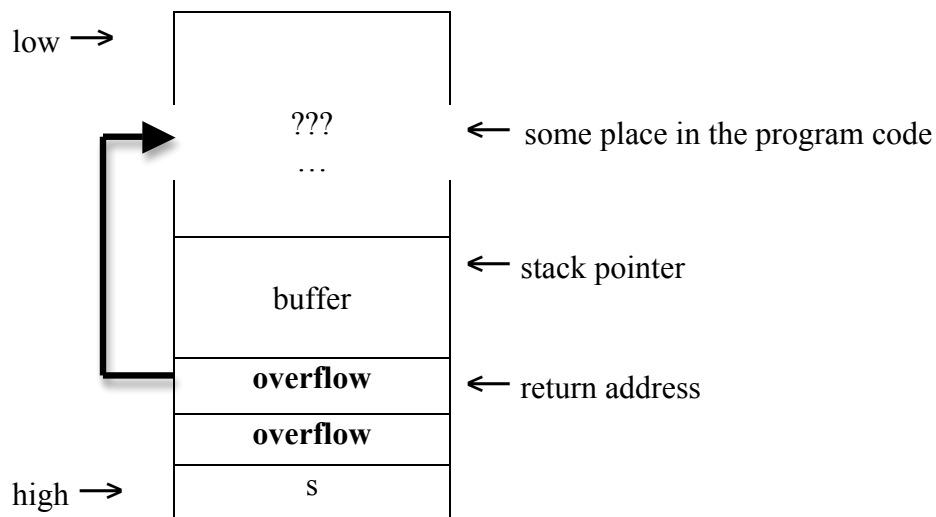


Figure 2.

Now, imagining that at another time, when the program was executed again, another buffer overflow (this time more malicious) occurred, which resulted in the memory layout shown in the following Figure 3.

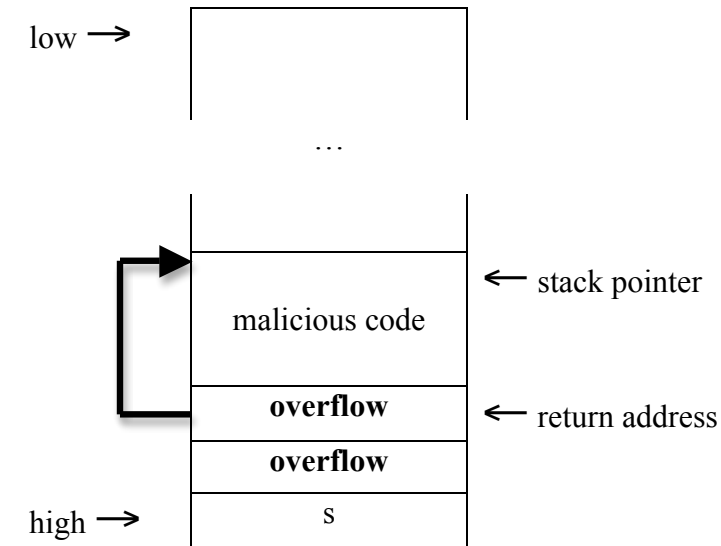


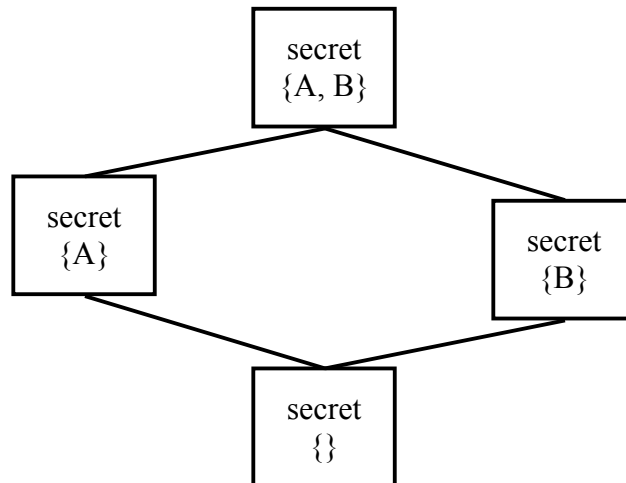
Figure 3.

Discuss three different options for mitigating or avoiding the above two types of buffer overflow attacks. Explain which option will work and will not work for which of the above buffer overflow attacks.

- 2. Explain the difference between how SQL injection attacks and cross-site scripting attacks work.**

3. Access control. For the following two policies, determine whether they are equivalent (i.e., users have same permissions in both policies). Explain your answer.

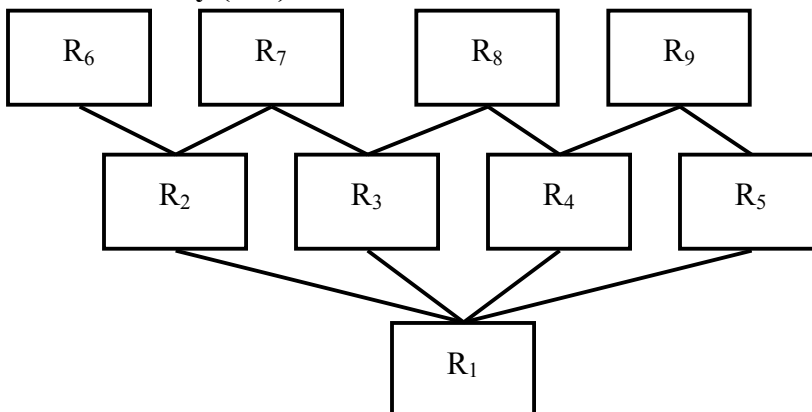
a. BLP policy.



Label	Object Classification	Subject Clearance
secret {A, B}	O ₃	U ₃
secret {B}	O ₄	U ₄
secret {A}	O ₂	U ₂
secret { }	O ₁	U ₁

b. Hierarchical RBAC policy

Role hierarchy (RH):



Permission-to-role assignment (PA):

permssn role	O ₁	O ₂	O ₃	O ₄
R ₁	read		append	
R ₂				append
R ₃				read
R ₄		read		
R ₅		append		
R ₆	append			
R ₇				
R ₈			read	
R ₉				

User-to-role assignment (UA):

user role	U ₁	U ₂	U ₃	U ₄
R ₁				
R ₂				
R ₃				
R ₄				
R ₅				
R ₆	X			
R ₇				X
R ₈			X	
R ₉		X		

The above two policies are equivalent: ___ Yes, ___ No

Because ...