**CS 4235/6035 QUIZ THREE (TAKE HOME)**

Spring, 2016

**Your Name**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Shujun Bian\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Your GTID**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_903172758\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Instructions:** Open book, open notes, no other sources.  No time limit.  *No collaboration*.  Please copy this document and type your answers after the question.  Try to preserve formatting in order to make grading easier.  Submit your quiz as a PDF on T-Square.  Best wishes!

**Due: 18 April, 10:00 PM**  Submit early to avoid last minute technical difficulties!

Hint: *One of the main purposes of this quiz is to make sure that students have read the textbook.*

[ One Point ] Regarding access control matrices, when we decompose a matrix by columns we get an:

Access control list.

[ One Point ] When we decompose an access control matrix by rows we get:

Capability tickets.

[ Two Points ] What are the two main properties of the BLP security model?

No read up: A subject can only read an object of less or equal security level. This is referred to in the literature as the simple security property (ss-property).

No write down: A subject can only write into an object of greater or equal security level. This is referred to in the literature as the \*-property1 (pronounced star property).

[ Two Points ] What are the three properties of a trusted system reference monitor discussed in the textbook?

Complete mediation, isolation and verifiability.

[ One Point ] Which kind of buffer overflow can overwrite a function’s return address pointer, allowing the attacker to take control of code flow?

Stack buffer overflow.

[ One Point ] What do we call a bit that indicates to a CPU that a page of memory should not contain executable code?

No-execute bit.

[ Two Points ] Explain in your own words the “return to system call” idea in chapter ten of the textbook.  What is its purpose?  How does it work?

It could allow the attackers injecting their malicious code and execute that code while avoid some restriction like non-executable stack. It changes the returning address of attacked program to some existing code on the system. It takes use of the buffer overflow to replace the saved frame pointer to some other suitable address meanwhile it also adds some values on the stack. So when the system call starts to execute, it would treat these values as parameters. It could even chains two library calls, usually the first call would be e strcpy(), so that it would copy some malicious shellcode from the non-executable buffer of attacked program to some other executable memory.

[ Two Points ] Suppose that malware that starts running as a limited user is able to use a system flaw to execute code as the root / system user.  This is an example of what?

Privilege escalation.

[ Two Points ] Define *incomplete mediation*.

The security rules are enforced on some access but not every access, which means some accesses are not checked against the access control mechanism.

[ Two Points ] Which Linux system call is used to “restrict a view of the file system to just a specified portion?”  (Quotation is directly from the textbook.)

The chroot system call.

[ Two Points ] What famous malware used a stack overflow in fingerd to open a shell on a remote system in order to propagate (among other propagation mechanisms)?

The Morris Worm.

[ Two Points ] What do we call malware that changes its own code in such a way that copies function the same but that the code is changed such that it is difficult for virus anti-malware software to detect it?

Polymorphic.