CS499 Second Examination

INSTRUCTIONS:

Email me (alex.groce@nau.edu) with subject: 499 SECOND TEST

And a message where the body has the format:

<login> answer1 answer2 answer3 answer4 answer5 answer6 answer7 answer8 answer9 answer10

e.g., I might send, if I were taking the test:

adg326 a a a a a a a a a a

Not following these instructions (wrong subject, wrong format of the message) will result in a 5 point penalty.

Now, the questions!

1. Which of the following is NOT TRUE?

a. Symbolic execution involves running a program with more "abstract" or algebraic values.
b. Symbolic execution requires programs to declare a loop bound, specifying how many times each loop can be run.
c. Symbolic execution has trouble scaling to long/complex program executions.
d. Symbolic execution is supported by DeepState.

2. A _weakness_ of static analysis, relative to dynamic analysis (testing) is:

a. It can never declare that a certain bug cannot happen.
b. It usually runs much, much, more slowly.
c. You have to build and execute the code for static analysis.
d. Static analysis tends to produce false positives, claiming a bug might exist when it really can't.

3. Which of these is true?

a. Some static analysis is applied every time you compile a program.
b. There are free static analysis tools available for various programming languages.
c. Static analysis is heavily applied to widely-used open source systems.
d. All of the above

4. Code coverage

a. Is an inherent measure of test goodness: tests with higher coverage always find more bugs.
b. Is not possible to compute for C and C++ programs, due to pointers.
c. Is an approximate, rough measure of test suite quality; but not covering important code is always bad.
d. Is the most useful output of a static analysis tool.

5. Mutation testing

a. Randomly selects some tests to run to see how many of your tests are needed to find a bug
b. Injects fake bugs into programs to see if a test suite can spot them
c. Is not applicable when you use a fuzzer to test a program
d. Is generally cheaper and easier to apply than measuring code coverage

6. CBMC expands to:

a. COBOL Businessman's Money Club
b. Complete Basic Model Checker
c. C Bounded Measurement Code
d. C Bounded Model Checker

7. Checking timing properties is often important for embedded code, but

a. It can be hard to fuzz for, because it means the thing under test may take a long time to run.
b. Whether a test passes or fails can be hard to predict
c. Can usually be ignored, because in practice bad inputs causing deadline misses are too rare to worry about
d. a and b

8. Embedded systems

a. Are probably unlikely to still be around in 2030, since they are being replaced by the Internet of Things
b. Are all around us, and can be safety critical or economically important
c. Are seldom written in anything but Java
d. Do not have particular problems with memory and pointer safety issues

9. DeepState has built-in interfaces to

a. AFL, libFuzzer, and symbolic execution tools
b. AFL, CBMC, and Amazon Web Services
c. AFL and VirtualBox
d. libFuzzer and the post office

10. Which of the following describes a desirable practice in testing a very critical embedded system?

a. Run lots of tests with sanitizers enabled to detect memory, thread, or other issues that may not normally cause a crash
b. Use a fuzzer to generate large numbers of potentially unexpected inputs, to make sure the system can handle unusual data
c. Apply good static analysis tools to look for bugs where fuzzers may have trouble generating the right inputs
d. All of the above