Quiz: Buffer Overflow Defenses

5 Questions, Answers follow the “About” page.

Author: Jedidiah R. Crandall, crandaj@erau.edu

This Document was Funded by the National Science Foundation
Federal Cyber Service Scholarship For Service Program:
Grant No. 0113627

Distributed July 2002

Embry-Riddle Aeronautical University • Prescott, Arizona • USA

1. Which of these can prevent a buffer overflow before the software is released?

A. Testing
B. StackGuard
C. Code Inspection
D. Anti-virus software

2. Which of these will anti-virus software prevent?

A. Known attacks on known vulnerabilities
B. Unknown attacks on known vulnerabilities
C. Attacks on unknown vulnerabilities
D. Careless software engineering practices

3. Which of these statements are true?

A. Languages like Java and Ada are less susceptible to buffer overflows
B. Programmers who use Java or Ada don't ever have to think about buffer overflows
C. Java has better performance in terms of speed than C
D. There are String libraries available for C/C++ that are safer than the standard libraries

4. Which of these tools would be appropriate during testing?

A. A static analysis tool
B. A dynamic analysis tool
C. StackGuard
D. A sledge hammer

5. Which of these buffer overflow preventions has a negligible performance overhead?

A. StackGuard
B. C compilers with automatic bounds checking
C. An operating system patch that disables execution of code outside of the code space
D. A C++ library for “limitless” buffers

About this Project

This presentation is part of a larger package of materials on buffer overflow vulnerabilities, defenses, and software practices.
For more information, go to: http://nsfsecurity.pr.erau.edu

Also available are:

- Demonstrations of how buffer overflows occur (Java applets)
- PowerPoint lecture-style presentations on an introduction to buffer overflows, preventing buffer overflows (for C programmers), and a case study of Code Red
- Checklists and Points to Remember for C Programmers
- An interactive module and quiz set with alternative paths for journalists/analysts and IT managers as well as programmers and testers
- A scavenger hunt on implications of the buffer overflow vulnerability

Please complete a feedback form at http://nsfsecurity.pr.erau.edu/feedback.html to tell us how you used this material and to offer suggestions for improvements.

Answers

1. A,C
2. A
3. A,D
4. B
5. C