

CPSC 331 - Operating Systems

Instructor Marc Corliss

Homework 7

Due: 12/5/07 (beginning of class)

1. Break the following monoalphabetic cipher. The plaintext consists of letters only. Each letter, digit, or punctuation symbol (‘;’, ‘:’, ‘,’, ‘ ’) in the ciphertext below maps to a letter. Spaces mean the same thing in both the encrypted and decrypted text; in both cases, they break the text into the individual words.

;0k ;9tk 03m eutk ;0k p3yiom m395 ;u ;3yg ur t3,a ;09,cm
ur m09nm 3,5 m0ukm 3,5 mk3y9,c p3q ur e3883ckm 3,5 g9,cm
3,5 p0a ;0k mk3 9m 8u9y9,c 0u; 3,5 p0k;0ki n9cm 03lk p9,cm
8o; p39; 3 89; ;0k uam;kim ei9k5 8kruik pk 03lk uoi e03;
rui mutk ur om 3ik uo; ur 8ik3;0 3,5 3yy ur om 3ik r3;
,u 0oia m395 ;0k e3ink,;ki ;0ka ;03,gk5 09t toe0 rui ;03;

4. Often one sees the following instructions for recovering from an attack:

- 1) Boot the infected system.
- 2) Back up all the files to an external medium.
- 3) Run the fdisk unix command to format the disk.
- 4) Reinstall the OS from the original CD-ROM.
- 5) Reload the files from the external medium.

Name two serious errors in these instructions.

5. Is there any feasible way to use the MMU hardware to prevent a buffer overflow attack within the stack? Explain why or why not?

6. Describe two techniques (besides, potentially the technique in the previous exercise) for preventing buffer overflow attacks in C and C++. Discuss the tradeoffs between these approaches.

7. Give some examples of languages that do not suffer from buffer overflow attacks. Why are buffer overflow attacks not a problem in these languages? Why do many programmers still use C and C++, which suffer from buffer overflow vulnerabilities?

8. What is a computer virus? Why do attackers write viruses (i.e., what can they gain)? How do viruses normally attack a system? What is the difference between a virus and a worm? Can a worm be harmful?