**CSE 484 In-class Worksheet #3**

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ UWNetID: \_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Email address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Student ID #: \_\_\_\_\_\_\_\_\_

Partner names for this activity: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Q1:** (In pairs): Sketch an attack string for an attack like this one which attempts to overwrite the return address of an earlier stack frame one byte at a time. You may use the diagram below to help think about this or illustrate your answer.

“… attackString%n”, attack code

RET

**Q2:** On your own, write down some defenses against code injection/buffer overflow vulnerabilities. Think inside the box – defenses that exist today or could be easily deployed – and also outside the box, such as defenses which would require rearchitecting operating systems or hardware?

**Q2.1:** Discuss in groups of 4: Given general purpose computers, are code injection vulnerabilities always going to inevitably be an important class of vulnerabiltiies?

**Q3:** Write down a brief description in words of how you could defeat StackGuard in the scenario where strcpy is called using a destination address stored in a local buffer. Refer to the diagram on the slide.

**Q4:** What was the best part of this class period?

**Q5:** What was a part of this class period that I could have improved?

**Q6:** Any other feedback?