

# **Labs and Exercises Using the Buffer Overflow Module Materials**

Susan Gerhart, gerharts@erau.edu

Embry-Riddle Aeronautical University • Prescott, Arizona • USA

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

©2002, Susan Gerhart, Jan G. Hogle. <http://nsfsecurity.pr.erau.edu>. Distributed July 2002.

---

## **Software Engineering**

1. Expand/apply the Checklist and Points to Remember on a C/C++ program from one of your courses
2. Assuming you're managing a software development shop, develop a risk analysis for a buffer overflow in one of your products
3. Assuming you operate a significant-sized web site, develop a risk analysis and mitigation plan for attacks exploiting buffer overflows
4. Download one of the defense tools, such as ITS4, and run it on some of your software. Or, run it on some open source software, even on itself.
5. Develop a test plan and test cases, then run test data, on software known to have buffer overflows.

## **Programming**

1. Experiment with both dangerous and safer versions of string libraries. Show how string functions cause buffer overflows.
2. Write exception handling to address buffer overflow types of exceptions, handling the exception as gracefully and safely as possible.
3. Switch programs with another student and change it to make buffer overflows occur, or show that buffer overflows are impossible.

## **Theory**

1. Prove that it's impossible to determine whether a program has a buffer overflow.
2. Develop a type system that can determine buffer overflows in a program in the language.

## **Management**

1. Risk analysis exercises as in software engineering
2. Develop a cost model for a company to determine the "time is money" equation - how much time should be spent testing and improving software practice versus the cost of a buffer overflow.

3. Examine the root causes and social implications of the thinking exhibited in the Scavenger Hunt questions.
4. Compare "buffer overflow" with Y2k for similarities and differences in costs, organizational responses, and effects on the public image of the computing profession.

## Other

- Assuming you want to become a Microsoft software engineering and MS gives those with security knowledge extra credit for employment, develop a personal education program enhance your proficiency in security (hint: use buffer "overrun", not "overflow")
- Assuming you're a programmer for one of those companies making a serious effort to improve its security public image, and you've just been caught by QA committing a buffer overflow error. Execute a crash course in causes and defenses to save your job.

## Labs on the web:

<http://www-net.cs.umass.edu/~brian/cs515/515-overflow.ppt>  
<http://sukka.jct.ac.il/~roman/tcp-ip-lab/admin/project.html>  
<http://www.cs.wm.edu/~lowekamp/classes/304/labs/buflab.pdf>  
<http://csapp.cs.cmu.edu/public/labs.html>  
<http://www.cs.berkeley.edu/~pattrsn/61CF00/labs/lab12.html>  
<http://www.cs.northwestern.edu/~pdinda/ics-f01/exploitlab.pdf>  
<http://isis.poly.edu/courses/cs392/labs/lab05/lab05.pdf>  
[http://www.cc.gatech.edu/classes/AY2002/cs6262\\_spring/lab2.txt](http://www.cc.gatech.edu/classes/AY2002/cs6262_spring/lab2.txt)  
<http://www.cs.wfu.edu/~fulp/CSC191/buffer.pdf>  
<http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/BufferOverflow/>

---

This document 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.