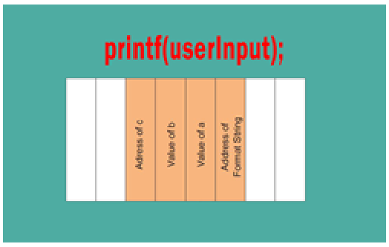
Format-String Vulnerability Lab

SEED Lab: A Hands-on Lab for Security Education

Overview



The learningrning objective of this lab is for students to gain the first-hand experience on format-string vulnerability by putting what they have learned about the vulnerability from class into actions. The format-string vulnerability is caused by code like `printf(user_input)`, where the contents of variable of `user_input` is provided by users. When this program is running with privileges (e.g., Set-UID program), this `printf` statement becomes dangerous, because it can lead to one of the following consequences: (1) crash the program, (2) read from an arbitrary memory place, and (3) modify the values of in an arbitrary memory place. The last consequence is very dangerous because it can allow users to modify internal variables of a privileged program, and thus change the behavior of the program.

In this lab, students will be given a program with a format-string vulnerability; their task is to develop a scheme to exploit the vulnerability. In addition to the attacks, students will be guided to walk through a protection scheme that can be used to defeat this type of attacks. Students need to evaluate whether the scheme work or not and explain why.

Lab Tasks (Description) (Video)

- **For instructors:** if you prefer to customize the lab description to suit your own courses, here are our Latex source files.
- **VM version:** This lab has been tested on our pre-built `SEEDUbuntu12.04` VM.

Recommended Time:

- Supervised situation (e.g. a closely-guided lab session): **2 hours**
- Unsupervised situation (e.g. take-home project): **1 week**

Files that are Needed

- vul_prog.c
- write_string.c

Helpful Documents

- (scut / team teso) Exploiting Format Strng Vulnerabilities
- Pradeep Padala. Playing with `ptrace`

SEED Project

- Home Page