15-213
Introduction to Computer Systems

Stacks and Buflab

Recitation 3
Monday September 21th, 2009

Today

- Schedule
- DataLab and Bomblab Questions
- Buflab and Stacks
- Buffer Overflow Example
- Exam Review

Schedule

- Today: Datalab handed back
- Tomorrow: Exam Review. Bring specific questions.
- Tomorrow, 11:59 PM: Bomblab due and Buflab available.
- Thursday: Exam
- Tuesday, Oct. 6: Buflab due

Questions about Datalab or Bomblab?

Buflab

Buflab

- Apply a series of five stack buffer overflow attacks on an executable file in order to modify the stack and change program behavior.
- Disclaimer: The purpose of this lab is to help you learn about the runtime operations of programs and understand the nature of this form of security weakness so that you can avoid it in your code. There are criminal statutes against using any form of attack to gain unauthorized access to any system resources.
- Commercial code is (usually) much more secure than the code in the lab.

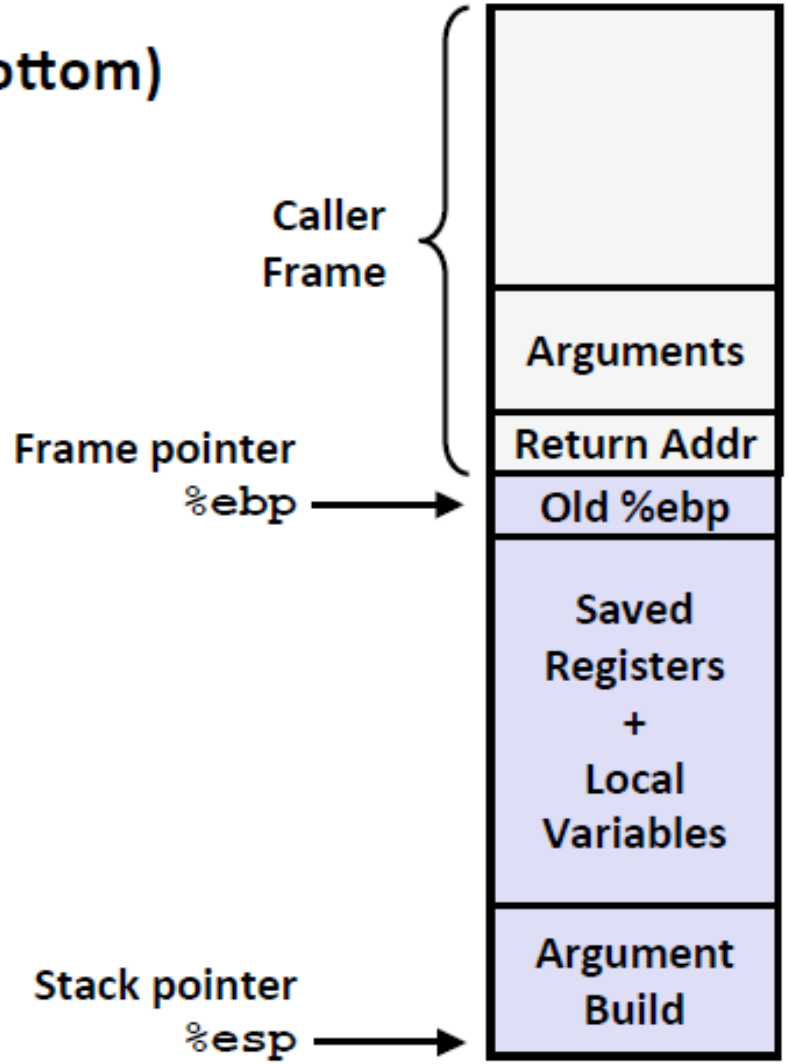
Buflab

- No penalty for wrong answers.
- You will need to know how the stack is set up and how it operates.
- Review the lecture slides and the textbook.
- Use GDB and objdump -d

IA32/Linux Stack Frame

- **Current Stack Frame ("Top" to Bottom)**
  - "Argument build:"
    Parameters for function about to call
  - Local variables
    If can't keep in registers
  - Saved register context
  - Old frame pointer

- **Caller Stack Frame**
  - Return address
  - Pushed by `call` instruction
  - Arguments for this call



Examples of Buffer Overflow Attacks

- The Morris Worm: Launched Nov. 2, 1988.
  - Exploited vulnerabilities in Unix.
  - Intended to merely gauge the size of the Internet, but caused infected computers to become unstable.
  - Infected approximately 10% of the 60,000 computers connected to the Internet, causing at least $10M in damage.
  - Prompted DARPA to fund the creation of the CERT Coordination Center at CMU.
  - Robert Morris, who created the worm, was sentenced to three years probation, 400 hours community service, and a $10,000 fine.

(Source: http://en.wikipedia.org/wiki/Morris_worm)

Examples of Buffer Overflow Attacks

- The SQL Slammer Worm: Launched Jan. 25, 2003
  - Exploited a bug in Microsoft's SQL Server and Desktop Engine database products.
  - 90% of vulnerable machines were infected within ten minutes.
  - Caused significant slowdowns globally, and even caused Internet services in all of South Korea to shut down for hours.

(Source: http://en.wikipedia.org/wiki/SQL_Slammer)

A very simple example of a Stack Buffer Overflow Attack: buf.c

Exam on Thursday

- Open book and open note, but you won't have time to look up every answer.
- Study past exams and know how to answer the questions, but remember that this exam may differ from past exams.
- Exam Review tomorrow: Question and Answer, so bring SPECIFIC questions.
- Any questions now?

Recap

- Schedule
- DataLab and Bomblab Questions
- Buflab and Stacks
- Buffer Overflow Example
- Exam Review