第五次小班课

计算机系统导论 (Class 9)

老师: 汪小林
助教: 陈东武

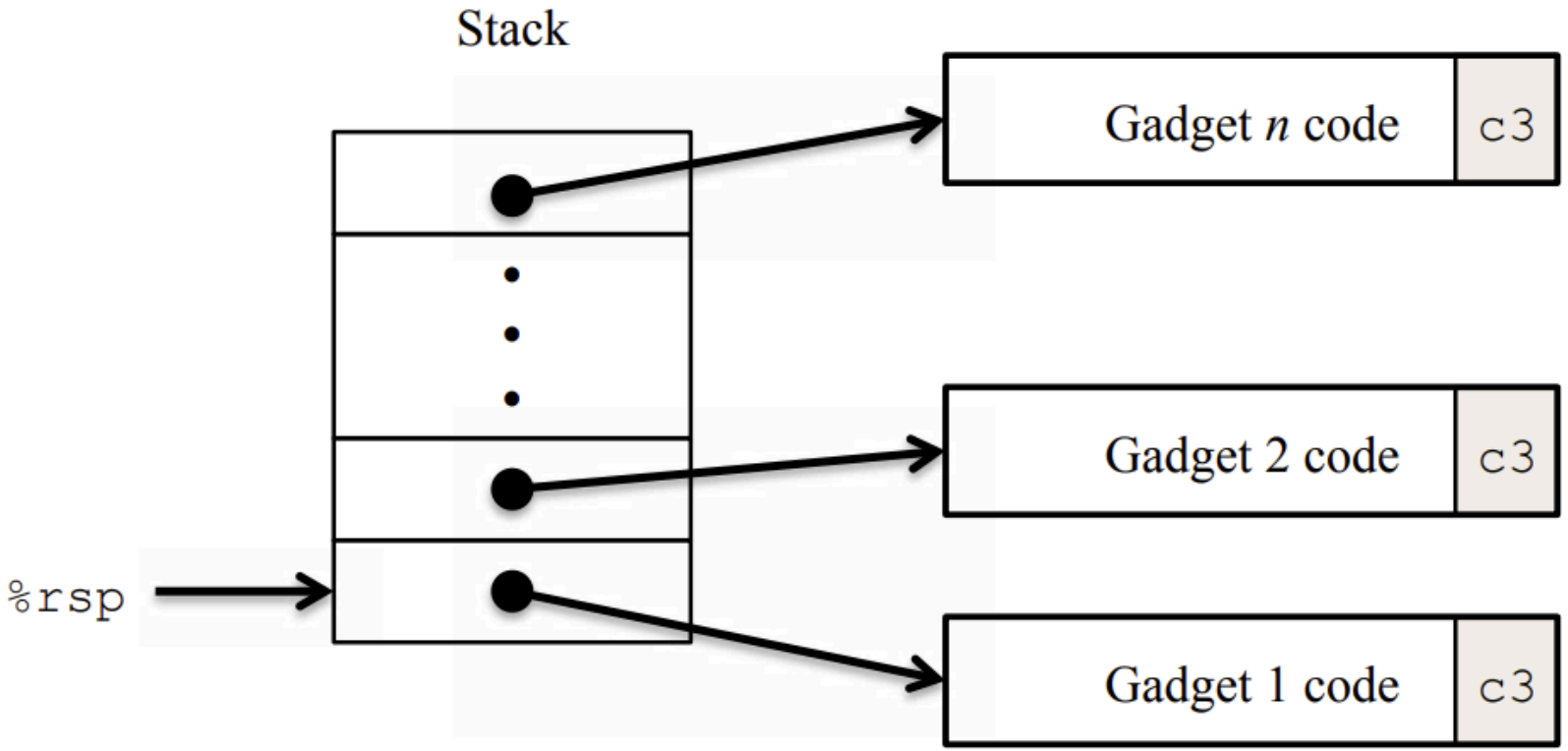
北京大学 信息科学技术学院

2024 年 10 月 16 日

Additional Comments

Exploiting Stack Buffer Overflows

- Code injection: inject the machine code and execute it.
- Return-oriented programming: use small **gadgets**, combine them by `c3`.
- You will implement these attacks in **attack lab**.



RISC v.s. CISC

- The table on page 249 is **the most important** part of this lecture.

CISC	RISC
Multiple formats for operands.	Simple addressing formats.
Operations can be applied to **both memory and register** operands.	Arithmetic and logical operations **only use register** operands.
Implementation artifacts **hidden** from machine-level programs.	Implementation artifacts **exposed** to machine-level programs.
Condition codes.	**No condition codes.**
Stack-intensive procedure linkage.	**Register-intensive** procedure linkage.
Easy for compiler.	Need support of advanced compiler.
Fewer code bytes.	**More code bytes.**
Currently dominates markets of **PC and server processors.**	Currently dominates markets of **embedded processors.**

Logic Design

- You are required to use HCL to describe circuits and fill out tables that organize instruction processing into phases.
- There are no expressions and assignments in HCL, just wires and signals.
- **Classic RISC pipeline**: fetch, decode, execute, memory, write back.

Copilot Tutorial

GitHub Education benefits

- GitHub Global Campus helps students, teachers, and schools access the tools and events they need to shape the next generation of software development.
  - Access https://education.github.com/discount_requests/application to apply for student benefits.

1. Secure your GitHub account with two-factor authentication.
2. Complete your GitHub billing information.
3. If your laptop can't locate or take photos, use a smartphone.
4. You may not use a VPN. Use the campus network whenever possible.
5. Follow the instructions. Take a photo of the student card and upload it.
6. It could work if you don't receive the email immediately. Wait for 3-7 days.

Usage of Copilot

- Install Copilot in VSCode extension marketplace.
- Log in with your GitHub account.

- It's **recommended** to use Copilot **properly** to help you with your lab work.
- Pretend this isn't a well-known assignment that millions of people have done.
- If you just generate all the code, it won't work ~~and pass the plagiarism check.~~
- You may design the code base and use it to complete some tedious work.

GNU Make Tutorial

Introduction to Makefile

- **Make** is a software tool that performs actions ordered by configured dependencies as defined in a configuration file called a *makefile*.
- Makefiles can contains *rules*, *variable definitions*, *directives*, and *comments*.
  - Each rule begins with a *dependency line*, consists of the *target* followed by a colon and optionally a list of targets, which are the rule's *prerequisites*.
  - A dependency line may be followed by a series of TAB indented command lines which define how to generate the target from the source files.
  - This commands are performed iff any prerequisite has a more recent timestamp than the target file or the target does not exist as a file.
- **Learn it further on real projects**, not in documentation or tutorials.

Exercise

```
char *get_line() {
  char buf[4], *result; gets(buf);
  result = malloc(strlen(buf));
  strcpy(result, buf);
  return result;
}
```

```
get_line:
  push    %rbx
  sub     $0x10, %rsp
  mov     %rsp, %rdi
  callq   4006a0 <gets>
  # ignore multiple lines
```

Procedure `get_line` is called with the return address equal to 0x400076. You type in 24 zeros and `12`.

- To what address does the program attempt to return? 0x3231.
- How many strings can you type in where the first 24 characters are zeros and the length is less than 32, so that the function still returns to the correct address? 1 or 7.
- Besides the potential for buffer overflow, what two other things are wrong with the code for `get_line`?

#thanks