Information Leakage

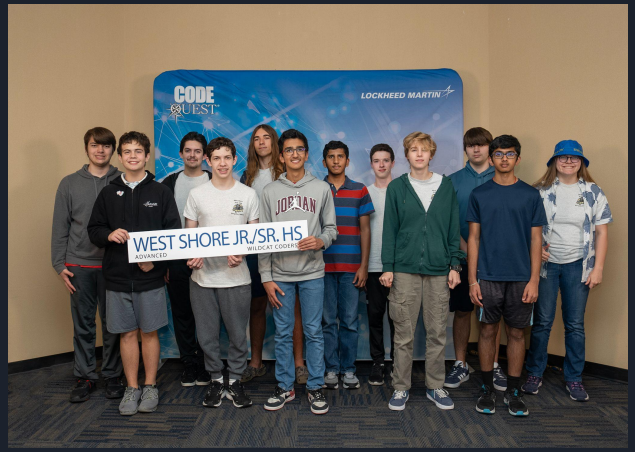
Level 0x0a

Quick Overview

- Events / Planning

Upcoming Events

- Code Quest
  - Saturday, March 1
  - Teams are 2-3 people
- Spring Break. March 17-21st
- Cyber Quest
  - March 29
  - Teams are 3-5 students
- We need to setup teams and get a list of who is going



Code Quest

- 4 Teams (2-3 students per team), 5th team is maybe / waitlist
  - Team name
  - Novice or Advanced
- Light breakfast, and lunch are provided
- Each team member can bring 1 computer, 1 monitor
- No cell phones, no cameras, no family members
- Lockheed Requirements
  - Bring IDs / Passports
  - Non-US citizens are allowed (need additional information for registration)
  - Liability Waiver and Photo Release
- Brevard County Public Schools
  - Field Trip Permission Form for BCPS

Limor Fried “Lady Ada”

- MIT EE and CS graduate
- Made hardware projects during college, open sourced design
  - ladyada.net
- Started selling hardware kits
- Create adafruit.com / Adafruit Industries
- Best guides / tutorials / instructions
- Open source hardware
- Maker movement

Format String Bug

- printf(user_controlled_variable)
  - “%p” = dumps out pointers / hex contents of regs / stack
  - “%s” = dumps out ASCII string of address in reg / on stack
- Discloses local variables placed on stack
- Discloses address of program code (defeating address randomization)

Information leaking because of a bug in the code

But what if code is correct…

Timing Attack

- Compilers and processors try to execute everything as fast as possible
- Libraries try to optimize, execute as fast as possible
- Memory usage tries to be efficient as possible

How do we determine length of a string in C? my_var = “Wild”; Link to GNUs strlen function

Address	0x0010	0x0011	0x0012	0x0013	0x0014
Value	0x57	0x69	0x6c	0x64	0x00
Letter	W	i	l	d	\0

What about strcmp()?

```
bool stringCompare(const void *a, const void *b, size_t length) {
  const char *ca = a, *cb = b;
  for (size_t i = 0; i < length; i++)
    if (ca[i] != cb[i])
      return false;
  return true;
}
```

Loops over entire string. Check to make sure each character is same between two strings, or else it exits and tells caller strings are different

Code Analysis

- stringCompare(“ABCDEx”, “ABCDEF”) takes 6 loops
- stringCompare(“ABxDEF”, “ABCDEF”) takes only 3 loops

```
bool constantTimeStringCompare(const void *a, const void *b, size_t length) {
  const char *ca = a, *cb = b;
  bool result = true;
  for (size_t i = 0; i < length; i++)
    result &= ca[i] == cb[i];
  return result;
}
```

Always take 6 loops, but it’s slower

Side channel attacks

- Power monitoring
- Acoustic monitoring (components can hum/ring, fans can kick on)
- Cache attacks

NOTE: The Raspberry Pi's broadcast frequency can range between 1Mhz and 250Mhz, which may interfere with government bands. We advise that you limit your transmissions to the standard FM band of 87.5MHz–107.9MHz (see Step 3) and always choose a frequency that's not already in use, to avoid interference with licensed broadcasters.

This AI can pick up passwords from the sound of your keystrokes

Your keyboard clatter could be giving away secrets

By Husain Parvez December 10, 2023 at 11:06 AM | 10 comments

Attributions

- https://www.adafruit.com/about
- https://en.wikipedia.org/wiki/Timing_attack
- https://www.techspot.com/news/101142-ai-can-pick-up-passwords-sound-keystrokes.html
- https://makezine.com/projects/raspberry-pirate-radio/