Intro. to Secure Programming
Study Groups at NCYU

Chih-Hsuan Yang(SCC)

zxc25077667@pm.me

April 20, 2021

About me

- 楊志璿
- NSYSU Information security club founder
- Resume
- Linux, Modern C++

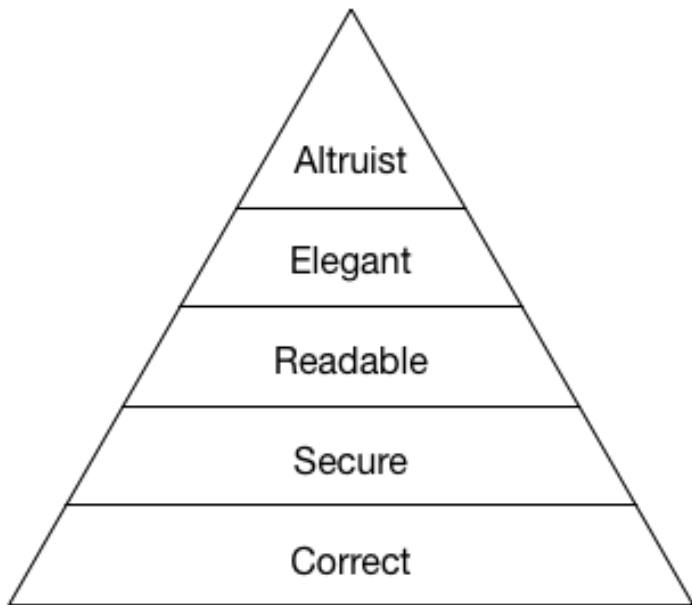# Outline

Background

Maslow's pyramid of code review

Maslow's pyramid of code review

- Correct：做到預期的行為了嗎？能夠處理各式邊際狀況嗎？即便其他人修改程式碼後，主體的行為仍符合預期嗎？
- Secure：面對各式輸入條件或攻擊，程式仍可正確運作嗎？
- Readable：程式碼易於理解和維護嗎？
- Elegant：程式碼夠「美」嗎？可以簡潔又清晰地解決問題嗎？
- Altruist：除了滿足現有的狀況，軟體在日後能夠重用嗎？甚至能夠抽離一部分元件，給其他專案使用嗎？

Programmer's qualities

Binary search

```c
int wrong(int *arr, size_t len, int target)
{
    int begin = 0, end = len;
    while (begin <= end)
    {
        int mid = (begin + end) / 2;
        if (arr[mid] == target)
            return mid;
        else if (arr[mid] < target)
            end = mid;
        else
            begin = mid;
    }
    return -1;
}
```

Binary search

```c
int correct(int *arr, size_t len, int target)
{
    int begin = 0, end = len;
    while (begin <= end)
    {
        int mid = (begin >> 1) + (end >> 1);
        if (arr[mid] == target)
            return mid;
        else if (arr[mid] < target)
            end = mid;
        else
            begin = mid;
    }
    return -1;
}
```
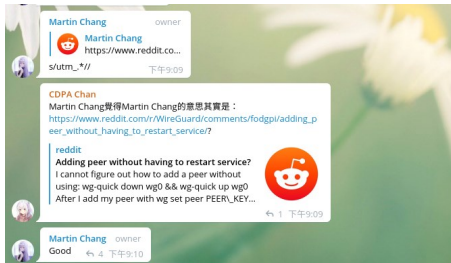
Binary search

- 1946 idea
- 1960 mathematical analysis
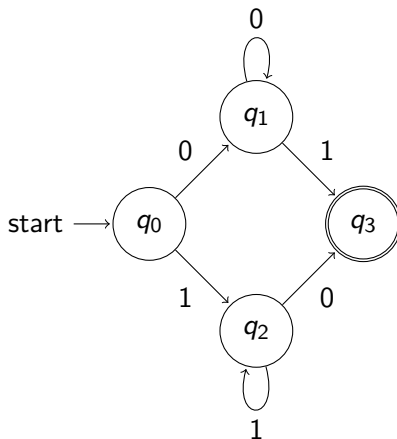- 1988 find bugs.

Donald Knuth

Although the basic idea of binary search is comparatively straightforward, the details can be surprisingly tricky.
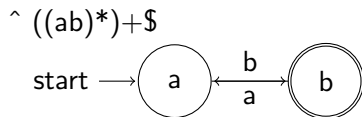
ReDoS

Regex

- Regular expression
- Finite state machine

Halting problem

^ ((ab)*)+$

start → (a) ⇄ ((b))
               b / a

Input

abababababababababababababa

Halting problem

The engine will first try (abababababababababababab) but that fails because of that extra a. This causes catastrophic bracktracking, because our pattern (ab)*, in a show of good faith, will release one of it's captures (it will "backtrack") and let the outer pattern try again.

- ▶ (abababababababababababab) - Nope
- ▶ (ababababababababababab)(ab) - Nope
- ▶ (ababababababababababab)(abab) - Nope
- ▶ (ababababababababababab)(ab)(ab) - Nope
- ▶ (abababababababababab)(ababab) - Nope
- ▶ (abababababababababab)(abab)(ab) - Nope
- ▶ (abababababababababab)(ab)(abab) - Nope
- ▶ (abababababababababab)(ab)(ab)(ab) - Nope
- ▶ . . .
- ▶ (ab)(ab)(ab)(ab)(ab)(ab)(ab)(ab)(ab)(ab)(ab)(ab) - Nope

Halting problem

$$NP\text{-Hard}$$

$$dp[0] = 1$$

$$dp[N] = \sum_{i=0}^{N} dp[i] + dp[N - i]$$

$$\sim \sum_{i=0}^{N} C_i^N = 2^N - 1$$