Intro. to Secure Programming

Study Groups at NCYU

Chih-Hsuan Yang(SCC)

zxc25077667@pm.me

April 25, 2021

About me

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

A book

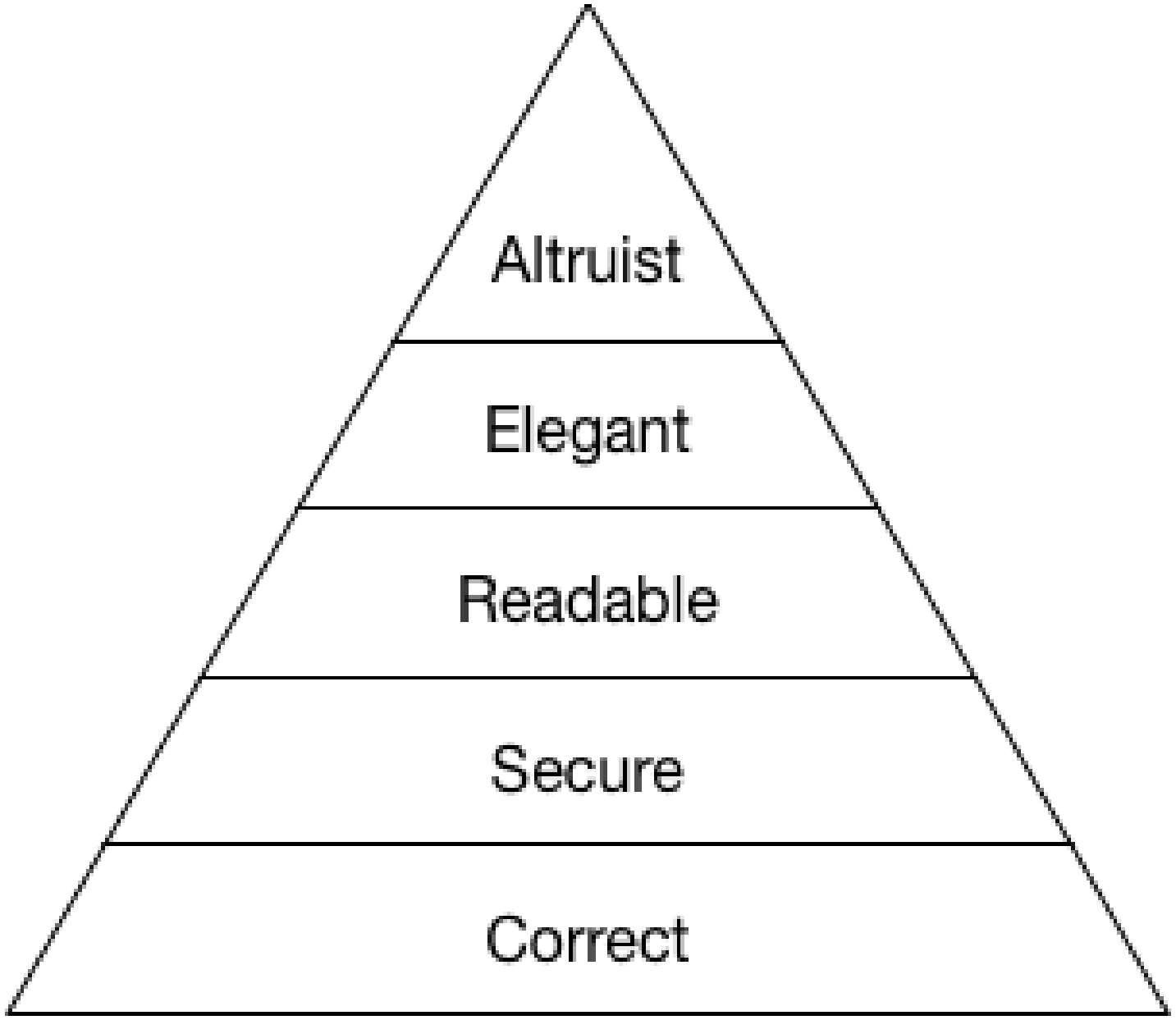
Secure Programming

Not hard, no much pages.

Outline

Background

Maslow's pyramid of code review



Maslow's pyramid of code review

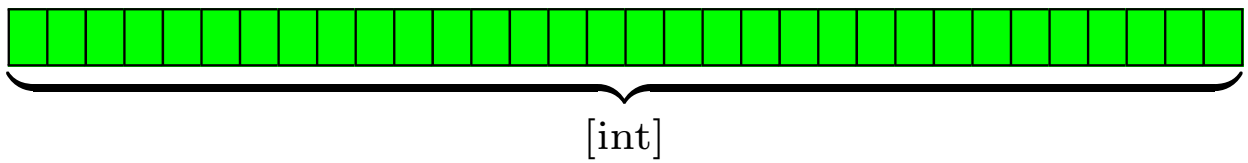
- Correct：做到預期的行為了嗎？能夠處理各式邊際狀況嗎？即便其他人修改程式碼後，主體的行為仍符合預期嗎？
- Secure：面對各式輸入條件或攻擊，程式仍可正確運作嗎？
- Readable：程式碼易於理解和維護嗎？
- Elegant：程式碼夠「美」嗎？可以簡潔又清晰地解決問題嗎？
- Altruist：除了滿足現有的狀況，軟體在日後能夠重用嗎？甚至能夠抽離一部分元件，給其他專案使用嗎？

Programmer's qualities

Arithmetic overflow

Data Model					
Type	LP32	ILP32	LP64	ILP64	LLP64
char	8	8	8	8	8
short	16	16	16	16	16
int	16	32	32	64	32
long	32	32	64	64	32
long long	64	64	64	64	64
pointer	32	32	64	64	64

Bits field



2's complement

Eg:

- 0x1234ABCD
- 0x00BADBAD
- 0xFFFFFFFF

Integer overflow

2002 FreeBSD

```
1 #define KSIZE 1024
2 char kbuf[KSIZE];
3 int copy_from_kernel(void *user_dest, int maxlen) {
4   int len = KSIZE < maxlen ? KSIZE : maxlen;
5   memcpy(user_dest, kbuf, len);
6   return len;
7 }
```

What if maxlen < 0?

Take maxlen as -1, try it!

Integer overflow

2002 External data representation (XDR)

```
1  void *copy_elements(void *ele_src[], int ele_cnt, int
       ele_size) {
2    void *result = malloc(ele_cnt * ele_size);
3    if (result == NULL)
4      return NULL;
5    void *next = result;
6    for (int i = 0; i < ele_cnt; i++) {
7      memcpy(next, ele_src[i], ele_size);
8      next += ele_size;
9    }
10   return result;
11 }
```

What if ele_cnt $= 10^{22}$, ele_size $= 10^{10}$?
Try it!

Binary search

```
1  int wrong(int *arr, size_t len, int target)
2  {
3      int begin = 0, end = len;
4      while (begin <= end)
5      {
6          int mid = (begin + end) / 2;
7          if (arr[mid] == target)
8              return mid;
9          else if (arr[mid] < target)
10             end = mid;
11         else
12             begin = mid;
13     }
14     return -1;
15 }
```

Binary search

```
1  int correct(int *arr, size_t len, int target)
2  {
3      int begin = 0, end = len;
4      while (begin <= end)
5      {
6          int mid = (begin >> 1) + (end >> 1);
7          if (arr[mid] == target)
8              return mid;
9          else if (arr[mid] < target)
10             end = mid;
11         else
12             begin = mid;
13     }
14     return -1;
15 }
```

Binary search

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

Donald Knuth

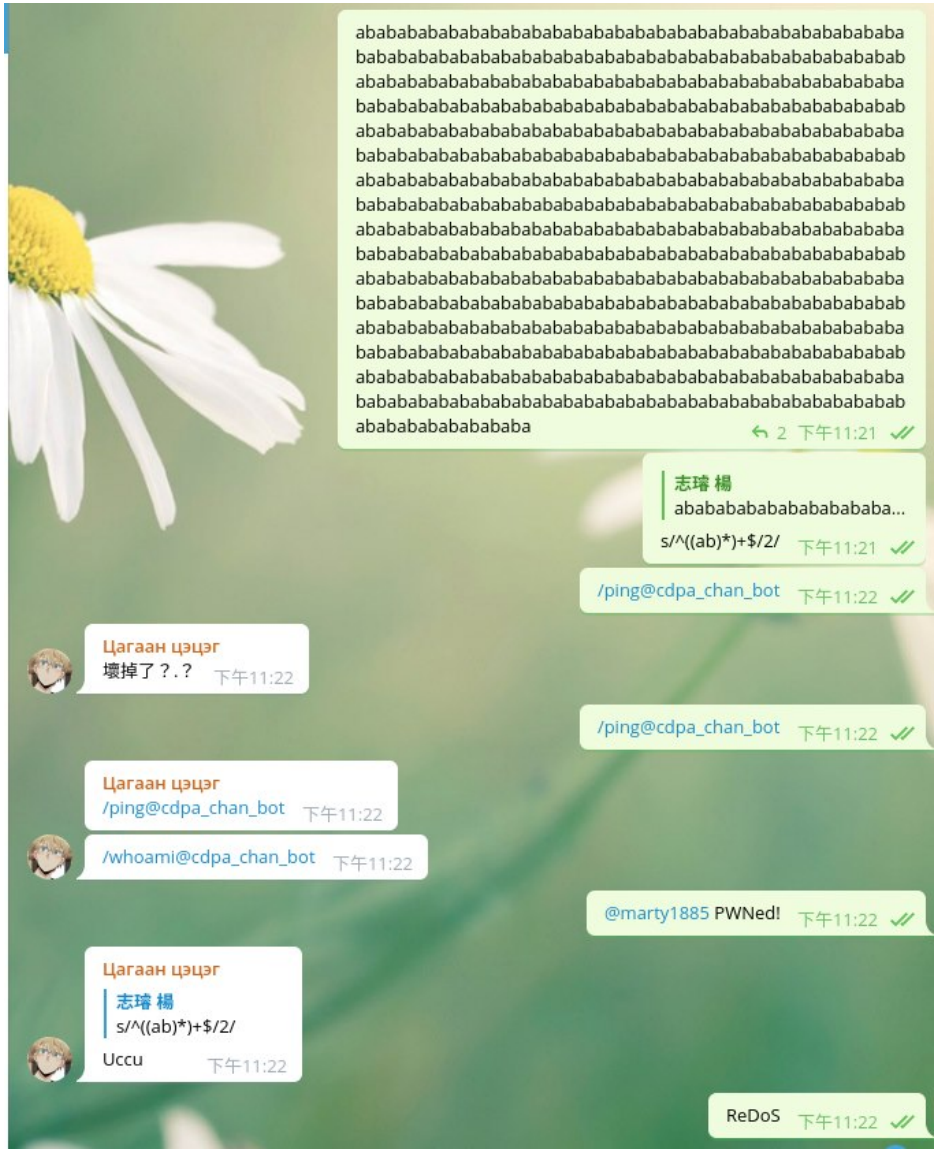
Although the basic idea of binary search is comparatively straightforward, the details can be surprisingly tricky.

Appendix here - Donald Knuth

- TEX
- The Art of Computer Programming (TAOCP)

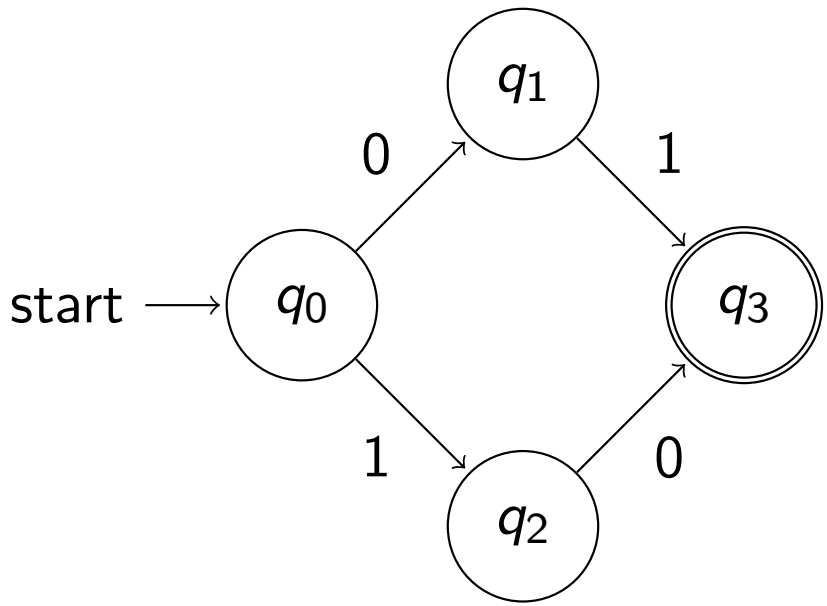
ReDoS


Martin Chang owner
Martin Chang
https://www.reddit.co...
s/utm_.*//
下午9:09
CDPA Chan
Martin Chang覺得Martin Chang的意思其實是：
https://www.reddit.com/r/WireGuard/comments/fodgpi/adding_peer_without_having_to_restart_service/?
reddit
Adding peer without having to restart service?
I cannot figure out how to add a peer without using: wg-quick down wg0 && wg-quick up wg0 After I add my peer with wg set peer PEER_KEY...
1 下午9:09
Martin Chang owner
Good
4 下午9:10


abababababababababababababababababababababababababa
babababababababababababababababababababababababababab
abababababababababababababababababababababababababa
babababababababababababababababababababababababababab
abababababababababababababababababababababababababa
babababababababababababababababababababababababababab
abababababababababababababababababababababababababa
babababababababababababababababababababababababababab
abababababababababababababababababababababababababa
babababababababababababababababababababababababababab
abababababababababababababababababababababababababa
babababababababababababababababababababababababababab
abababababababababababababababababababababababababa
babababababababababababababababababababababababababab
abababababababababababababababababababababababababa
babababababababababababababababababababababababababab
abababababababa
2 下午11:21
志琦 楊
abababababababababa...
s/^((ab)*)+$/2/
下午11:21
/ping@cdpa_chan_bot 下午11:22
Цагаан цэцэг
壞掉了？.？
下午11:22
/ping@cdpa_chan_bot 下午11:22
Цагаан цэцэг
/ping@cdpa_chan_bot 下午11:22
/whoami@cdpa_chan_bot 下午11:22
@marty1885 PWNed! 下午11:22
Цагаан цэцэг
志琦 楊
s/^((ab)*)+$/2/
Uccu
下午11:22
ReDoS 下午11:22

Regex

- Regular expression
- Finite state machine



Regex basic

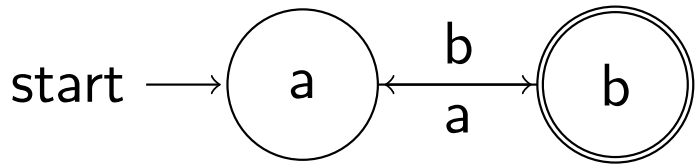
Regex 101

Let's try:

- A brown fox jumps over the lazy dog.
- Student ID.
- Binary search code.
- Email.

Halting problem

^ ((ab)*)+$



Input

abababababababababababa

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
- (abababababababababababab)(ab) - Nope
- (abababababababababababab)(abab) - Nope
- (abababababababababababab)(ab)(ab) - Nope
- (abababababababababababab)(ababab) - Nope
- (abababababababababababab)(abab)(ab) - Nope
- (abababababababababababab)(ab)(abab) - Nope
- (abababababababababababab)(ab)(ab)(ab) - Nope
- ...
- (ab)(ab)(ab)(ab)(ab)(ab)(ab)(ab)(ab)(ab)(ab)(ab) - Nope

Halting problem

$$dp[0] = 1$$

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

$$\sim O(3^N)$$

ReDoS

So, please check what you did.
User provides regex should have a timeout threshold.
Don't believe the user inputs.

RAII

- Resource Acquisition Is Initialization
- Bjarne Stroustrup
- Constructor, destructor
- Don't memorize.

RAII

lifetime

RAII

objects, files, sockets, locks

RAII

exceptions

Memory safe

Buffer overflow

sample code.

Buffer overflow

Try some code.
strcpy, strncpy

Buffer overflow

bof on stack

Buffer overflow

canary

Memory leakage

sample code

Memory leakage

Try some codes. new, delete.

Memory leakage

Garbage Collection

Memory leakage

RAII

Call out to other routines

SQL injection

not checking, string concatenation

Command line injection

not checking, don't call commands directly.

Others

Language features

Strong Type, week type, inheritance

Passwords

hash