Old school code audit?

SUSE Hackweek 10

Shawn the R0ck

Oct 12 2013

whois

NATIONAL SECURITY AGENCY
NSA Spying Confirmed
at&t
EFF
I SUPPORT FREEDOM ONLINE
BIG BROTHER IS WATCHING YOU
SURVEILLANCE IS SECURITY
NATIONAL SECURITY AGENCY
ALL YOUR DATA

Old good hacking days?

strcpy(fucked, buf, xXx);

1990s:

grep strcpy *.c

```
        Hack Construction Set //
           By Cyborg

              MAIN      12/12/87

    LBBS COMM.    D:47    F:1     02.1%
    N.C. PBX      D:167   F:0     00.0%
    XLNT.PBX      D:113   F:0     00.0%
    X-PRESSTEL    D:116   F:3     02.5%
    EMPTY         D:0     F:0     00.0%
    ITT           D:341   F:2     .8.6%
    BUDGET 950    D:10    F:0     00.0%
    GNU.ITT       D:26    F:0     00.0%
    EMPTY         D:0     F:0     00.0%

    [RET] [ESC] [SPACE] [D]elete <->

 CONNECT  CODE  WAIT 00  DISK  HUNGUP
```

printf(s_as_string);

around 2000:

grep –E –e ‘printf\s*\([^”]+[,\)]’ *.c

Audit was never easy as you think

Let's talk about file, permission.....

- 8 400 r-------- Owner may read
- 7 200 -w------- Owner may write
- 6 100 --x------ Owner may execute
- 5 040 ---r----- Group may read
- 4 020 ----w---- Group may write
- 3 010 -----x--- Group may execute
- 2 004 ------r-- Everyone else may read
- 1 002 -------w- Everyone else may write
- 0 001 --------x Everyone else may execute

More default polices?

GNU/Linux: use gid of the creating process(you can change this policy in mount options)

*BSD: use gid of the parent directory

Hard link example:

```
----------------------------------------
echo 'hello hard link!'  > test.log
ln test.log my_hardlink
----------------------------------------
```

test.log and my_hardlink are only one inode which contains the same content. The name and inode pair will be removed permanently(really?) only if the link count of its inode equal to zero.

HOWTO?

*Kernel will give you anwser:

kernel/include/linux/fs.h

```
struct inode {
...........
unsigned int    i_nlink;
...........
};
```

Exceptional handler

OK. You thought you are a good programmer. But...maybe you are just another fuc*ing monkey coder. Just don't realize what you're doing is fuc*ing wrong........

E.g:

```
Int ret = read(fd, potential_threat, size_is_l33t);
if( ret == -1){
………………. // that's it?
```

Read everything even something bad happened. End conditions are:

- ---
- read all len bytes(return len) or EOF is reached(return zero).
- ---
- And, execeptional handling:
- ---
- return a value less than len, re-calculate the buffer and number
- of bytes haven't read yet, then reissue read() again.
- return -1 and errno=EINTR, it's signal break before read anything.
- return -1 and errno=?, loop terminates
- ---

```
void read_all(int fd, void *buf, size_t len)
{
        ssize_t ret;
        while (len != 0 && (ret = read(fd, buf, len)) != 0) {
                if (ret == -1) {
                        if (errno == EINTR) /* EINTR = signal break, EAGAIN = no data currently available */
                                continue;
                        perror("read");
                        break;
                }
                len -= ret;
                buf += ret;
        }
}
```

More sides of the desert of the real

Standard I/O functions: good, popular, etc....

fflush() is ensure that the user-space buffer is written out to the kernel...just the kernel...then fsync() is ensure that the kernel buffer is written out to disk.

sync()? Well, that's too old school?

Hackweek 10

Awesome week!

* Hack anything you want

* Just boring code audit? No shit--->

* Telco sec shit are looks awesome

Step-1: Software defined radio-->listen to fm-->scan specific frequency-->locating airplane's info by Mode S transsmisson-->IR detection? well, I can't tell.

Step-2: Telco network protocol working with TCP/IP in one fuc*ing device....catch any info in the air, and in the wire

Gratitude

* SUSE gave us a week to think who we are! Very philosophical!

* People who was inspired by Phrack and underground spirit

* Bo Yang, fuc*ing awesome technical(note: not philosophical;-)) hacker I've rarely to met

* My neurons, I couldn't do anything without their commitment. No kidding;-)

***

Questions?

This is where we are............

Dude, keep hacking is our only choice to be alive