Secure Systems Engineering

Chester Rebeiro

Indian Institute of Technology Madras

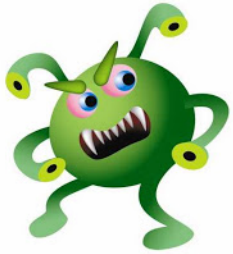
CR

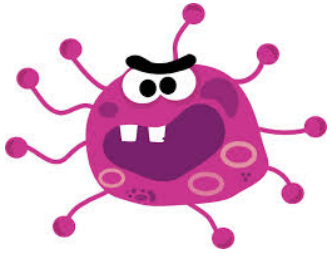
Secure Systems

- Computer systems can be considered a closed box.
- Information in the box is safe as long as nothing enters or leaves the box.

Systems Still Secure

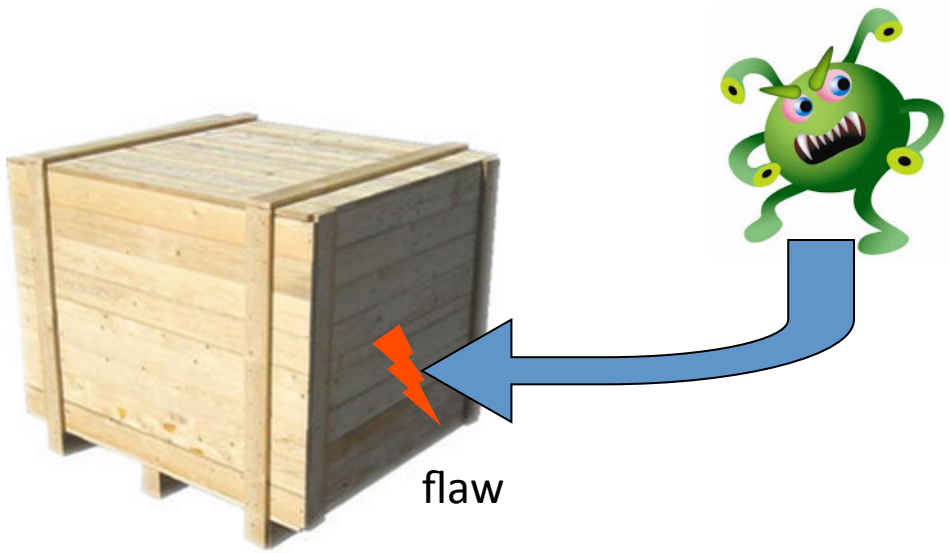
- Even with viruses, worms, and spyware around information is still safe as long as they do not enter the system





Vulnerability

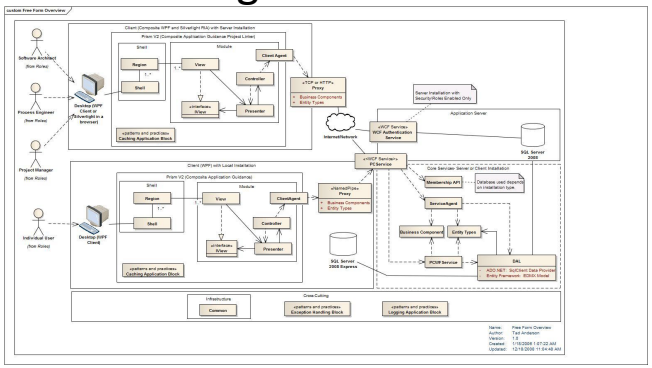
- A flaw that an attacker can use to gain access into the system



Flaws that would allow an attacker access a system

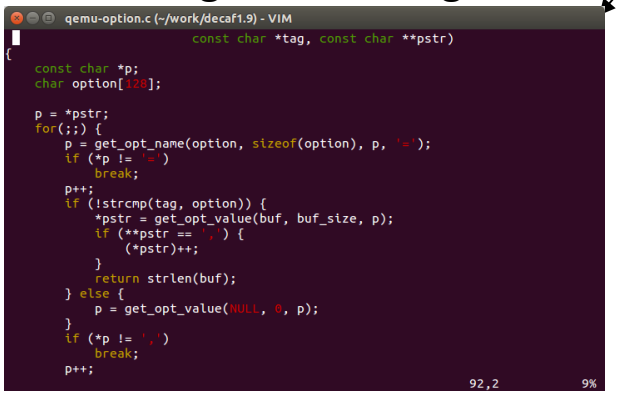
The attacker just needs one flaw … any flaw!!!

Design Flaws



flaw

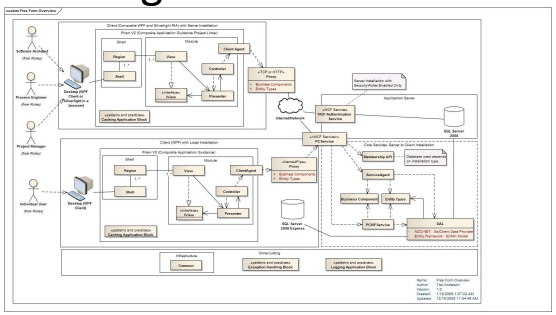
Bugs in the Program



The Human factor

You don’t need to be a granny to get fooled ☹

Design Flaws



flaw

The human factor

Gmail

RE: Document

Jean-Luc [redacted]
To: Chester Rebeiro [redacted]

Dear Chester,
I didn't receive anyting from you
Regards
Jluc

De: "Chester Rebeiro" [redacted]
À: "siddharth [redacted] gmail.com>
Envoyé: Jeudi 12 Septembre 2013 02:32:28
Objet: Document

Hi,
Did you receive the documents which I have sent earlier?
If not, I have re-uploaded them on my Google drive.
Click Here, I will upload rest of the documents soon.

Regards,

Bugs in the Program

qemu-option.c (~/work/decaf1.9) - VIM

```
                        const char *tag, const char **pstr)
{
    const char *p;
    char option[128];

    p = *pstr;
    for(;;) {
        p = get_opt_name(option, sizeof(option), p, '=');
        if (*p != '=')
            break;
        p++;
        if (!strcmp(tag, option)) {
            *pstr = get_opt_value(buf, buf_size, p);
            if (**pstr == ',') {
                (*pstr)++;
            }
            return strlen(buf);
        } else {
            p = get_opt_value(NULL, 0, p);
        }
        if (*p != ',')
            break;
        p++;
                                                    92,2          9%
```

Program Flaws

- In application software
  - SQL Injection
- In system software
  - Buffers overflows and overreads
  - Heap: double free, use after free
  - Integer overflows
  - Format string
- In peripherials
  - USB drives; Printers
- In Hardware
  - Hardware Trojans
- Covert Channels
  - Can exist in hardware or software

These are not really program flaws.

Secure Systems Engineering

Approach 1: Design flawless systems

eg. SeL4

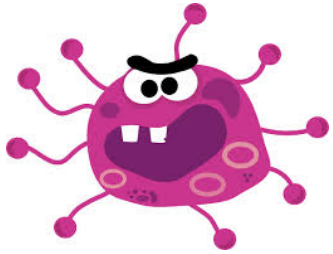
(Not easy to develop these systems in a large scale)

Static analysis /
Formal Proof Assistant
eg. COQ

Secure Systems Engineering

Approach 2: Make it difficult for the attacker

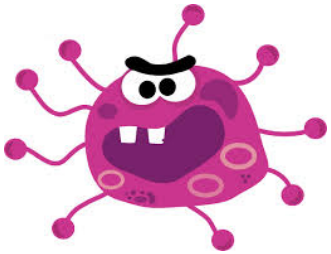
Develop systems that are secure in spite of flaws (detect attacks)



Secure Systems Engineering

Approach 3: Isolate systems : sandbox environments, virtual machines, trusted environments (trusted computing)

Takes care of the human factor as well



Course Structure

Part 1

- Programming flaws that have been exploited
- Design the System where the flaw no longer can exist
- Make it difficult for the attacker to mount an attack

Part 2

- Trusted Computing

Part 3

- Attack / Vulnerability / Malware detection

CR

What to expect during this course

- Deep study of systems:
  - Software
    - Assembly level
    - Compiler and OS level

    (Programming assignments in class and homework)
  - Hardware
    - Some computer organization features
- Analysis techniques
    - Static, dynamic analysis / symbolic execution
    - Statistical analysis techniques and some ML

    (Programming assignments for homework)
- Course Project & Reading assignment

CR

Expected Learning Outcomes

- Understand the internals of malware and other security threats
- Evaluate security measure applied at the hardware, OS, and compiler
- Understand trade offs between performance and security

CR

Grading

Quiz 1 : 15 marks

Quiz 2 : 20 marks

Endsem : 15 marks

Assignments, project : 40 marks

In class assignments / tutorials : 10

Dates as per academic calendar

CR

Schedule

- G slot

  ~~Monday : 12:00-12:50~~

  Wednesday : 16:50-18:30

  Thursday : 10:00-10:50

  Friday : 9:00-9:50

Move Monday 12:00-12:50 to Wednesday 17:40-18:30 ???

Laptop day!

Need updated Ubuntu laptop (32 or 64 bit);

You could also use an Ubuntu virtual machine

CR

Websites and Communication

- Reference Textbooks

  mostly research papers; will be provided as per topic

- For slides and schedule

  http://www.cse.iitm.ac.in/~chester/courses/17o_sse/

- For communication : google groups

  invitations will be sent to your smail account

  (please mail me or the TAs if you don't get an invite)

- For assignment submissions

  IITM moodle

CR