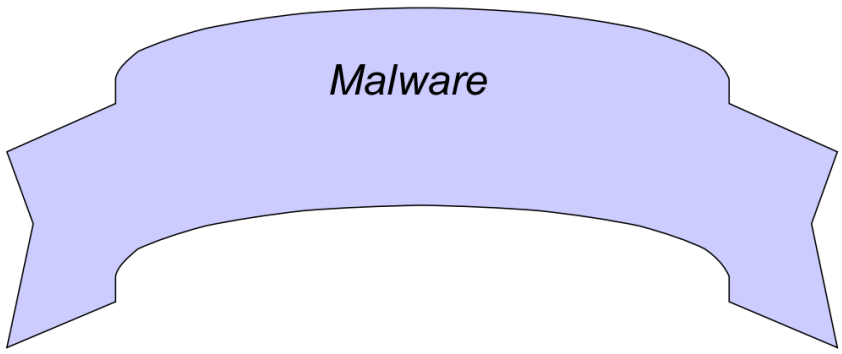


Logic Bombs

是一段 code

Logic Bombs and Viruses and Worms

當某 condition 發生時，會報行此 code，

Trojans

Key Logger

記錄使用者的所有輸入

Precautions：避免 login in Public PC visits

URL Injection

navigate 到錯的 web, domain....

Browser Hijacker

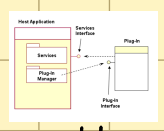
alters browser's settings

Redirection

file directly maps DNS addresses

Self-Protection Mechanisms of Browser Hijackers [PCSTATS]

Add-on



- plug-in
- extension：{add / modify the behavior，seen as part of the browser
  - toolbar
- theme

Binder

多個 files —combines into→ one host file

start the host ——→ 自動 decompressed & launched

Dropper

入侵
- Single stage：全含在 Dropper 內
- Two stage：Dropper 起動時才去下載 malware

Trojan Horse

- a useful software
- a standalone program

Spying functions

backdoor functions

網頁掛馬

利用漏洞，在 visiting website 時偷偷下載並 run

Create iframe with size 0

Spyware

Adware

Spyware and Pop-up Ads

Routes of Infection

- Masquerade
- Bundled with Shareware
- Through Trojan Horse

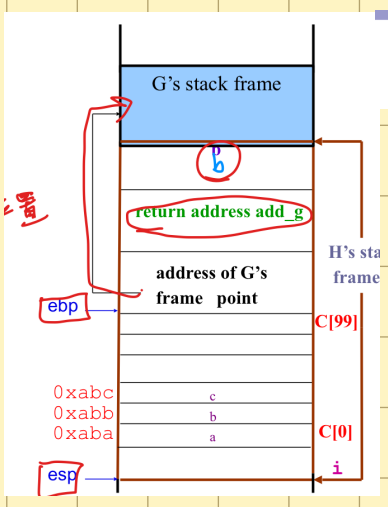
Worm

BOA

Attacking Program Bugs

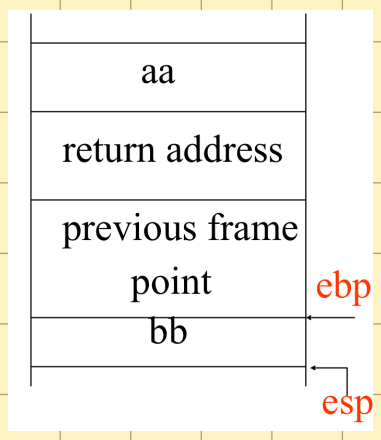
Why Buffer Overflow Attacks Are So Dangerous?

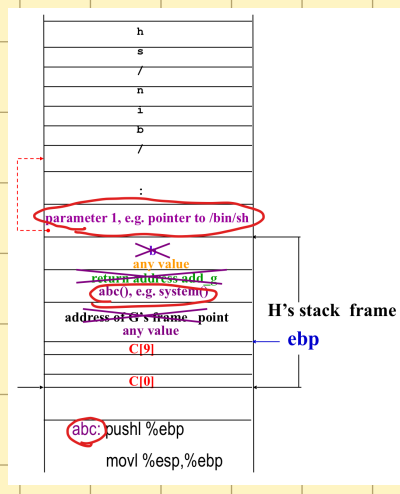
Stack Smashing Attacks



Injected Code:

Return-into-libc Attacks





Heap/Data/BSS Overflow Attacks

Function Pointer Attacks

Countermeasures of Buffer Overflow Attacks

Array Bounds Checking

Non-executable Stack/Heap

Safe **C** Library

Compiler Solution

StackGuard

RAD

Type Safe Language

Static Source Code Analysis

Anomaly Detection

Randomization of executable Code

Virus [Internet Security Professional Reference]

Virus

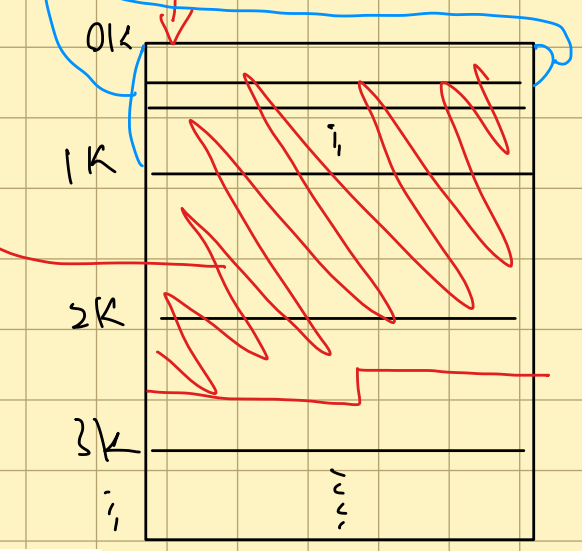
- 一段可 insert 入 a program 的 code
- 可複製自己到多個 program
- 無法自行 run，need host program

WIN32 PE Infection

Portable Executable (**PE**) Format

IMAGE_OPTIONAL_HEADER

- **AddressOfEntryPoint**
  - 執行 a point to the first function of image
- **ImageBase**
  - 以 64K byte base
    - DLL start 0x10000000
    - app " 0x00400000
    - Windows CE start 0x00010000
- **SectionAlignment** default: page size
- **FileAlignment** default: 512, 512 ~ 64K
- **SizeOfImage**
- **SizeOfHeaders**



File < Data < Section < Image

IMAGE_SECTION_HEADER

VirtualSize

SizeOfRawData

VirtualAddress

PointerToRawData

IMAGE_SCN_CNT_CODE 0x00000020	The section contains executable code.
IMAGE_SCN_CNT_INITIALIZED_DATA 0x00000040	The section contains initialized data.
IMAGE_SCN_CNT_UNINITIALIZED_DATA 0x00000080	The section contains uninitialized data.

Loading Process

Inject Virus

The Evolution of Media Used by Viruses to Spread Themselves

BBS, email, sharing files, USB

Methods to Avoid Detection

x64 病毒

Windows Fileless Malware

Ways to Run Code without Using