







作品附件

大學專案成果		
作品名稱	使用技術	頁碼
Dark Killer	Android SDK、Java Multithreading、Java Socket	1
Random It	Visual Basic、MySQL	2
彩色泡泡	Java Multithreading	3
研究所系統開發		
DNS Packet Tampering	Linux Kernel Module、Kernel Netfilter Framework	3
Android 惡意軟體開發	Java Server Socket、Android SDK	4
TEMU_ANTS	Python Script、Docker、C	4
分散式惡意軟體分析系統	Java、Cuckoo Sandbox	5
碩士論文	QEMU+KVM、Windows API hooking、x64 Assembly	5

作品說明

Android Game - Dark Killer

開發理念	目前市面上的手機 APP 遊戲，種類偏向於單機遊戲或是網路連線遊戲，較少桌遊類型的互動性遊戲，我們創造出擁有極高互動性，且舒適使用、容易上手之桌遊手機 APP 遊戲。	
功能特色	<ul style="list-style-type: none"> ◇ 使用者互動性高、簡單易用，容易上手 ◇ 不須倚靠 3G 網路，以行動基地台與 Wifi 連結方式進行遊戲 ◇ 身歷其境的音效及動畫效果 	
使用技術	Android SDK、Java Multithreading、Java Server & Client Socket	
負責工作	此作品為 5 人之合作專案，我負責系統架構設計與 80% 程式撰寫	
系統截圖	 <p>Figure 1 遊戲進入畫面</p>	 <p>Figure 2 開始畫面</p>
	 <p>Figure 3 人物說明</p>	

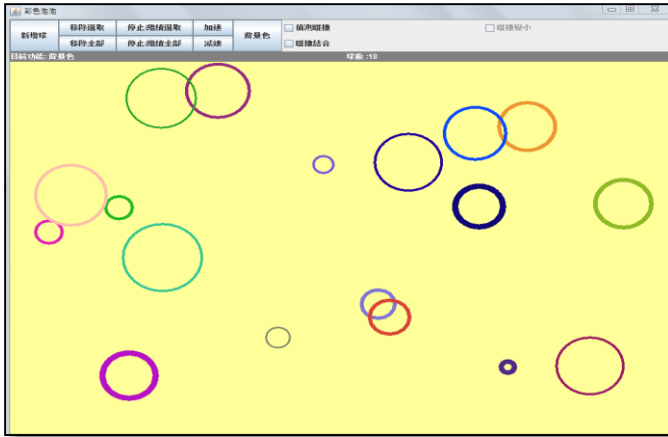
			
			

Random It - 自動點餐推薦系統

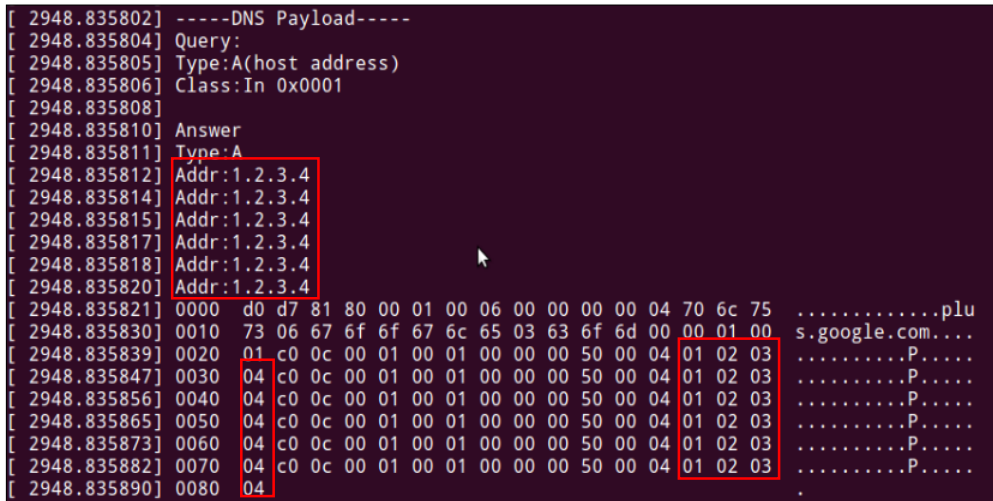
目標	鑒於中央大學學生每天面臨不知道要吃什麼的困擾，我們運用 VB 語言為中央大學量身打造食物目錄統合，解決同學不知道要吃什麼的煩惱。
系統功能	隨機推薦【早餐】、【午晚餐】店家與菜色，同時提供價格比對與查詢，再加上有趣的【菜餚格鬥小遊戲】增加使用者趣味性。
使用技術	MySQL、Visual Basic
系統截圖	

Figure 10 VB 實作餐點推薦系統

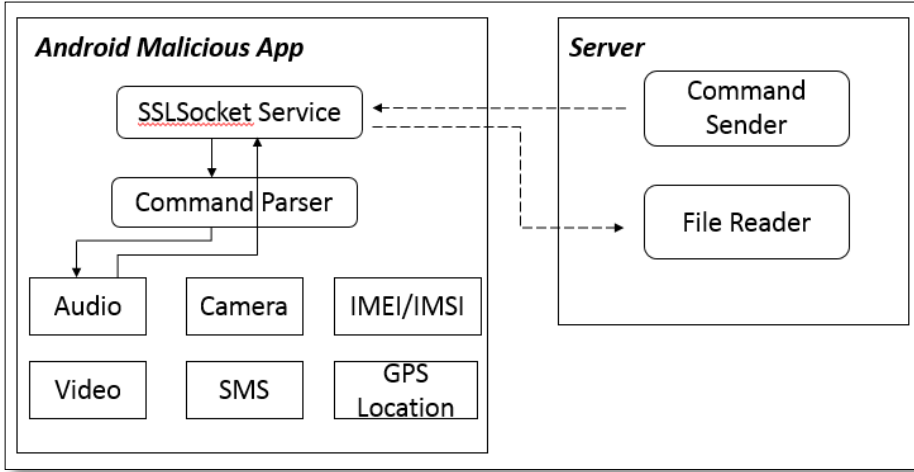
彩色泡泡

目標	模擬作業系統中 Multithreading 處理模式，實作程式
系統特色	如 Windows 螢幕保護程式般可產生多種顏色大小的泡泡，並可選擇【碰撞結合】、【碰撞縮小】、【加速】、【減速】等功能。
使用技術	JAVA Multithreading
系統截圖	 <p>Figure 11 Java 實作 Multithreading 的彩色泡泡</p>

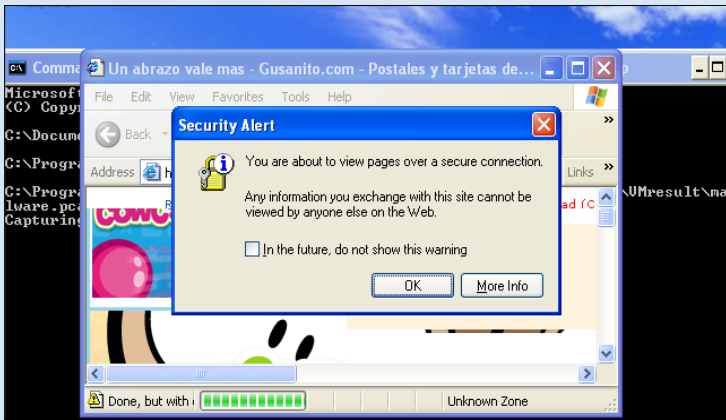
DNS Packet Tampering - A self-made linux kernel module

目標	撰寫 Linux kernel module(LKM)用以攔截網路封包並竄改其內容
系統功能	攔截 DNS response packet，並竄改 answer IP 為 1.2.3.4
使用技術	LKM、Kernel Netfilter Framework
系統截圖	 <p>Figure 12 竄改 DNS Answer IP 為 1.2.3.4</p>

Android 惡意軟體實作

目標	模擬駭客撰寫的手機惡意軟體，實作一個 Android 上惡意 App
系統功能	盜取 ISMI/IMEI、竊聽、偷照、竊取 SMS、傳送 Forged GPS
使用技術	Java Server Socket、Android SDK
系統截圖	 <p>Figure 13 惡意軟體系統架構圖(以竊聽為例)</p>

TEMU_ANTS - A Dynamic Malware Analysis System

目標	利用 docker 與 python 結合 TEMU 撰寫自動化程式執行惡意軟體行為側錄
系統功能	透過 script 自動化執行 TEMU，包括:啟動 TEMU、移動滑鼠點擊、螢幕截圖、移動大量 trace 檔案，並將整套系統製作成 docker image
使用技術	Python、Docker、C
負責部分	此為四人合作之系統，我負責實作 hooked Windows APIs 程式碼
系統截圖	 <p>Figure 14 Windows XP 內惡意軟體執行截圖</p>

Cuckoo Sandbox - A Distributed Malware Analysis System

目標	將現有 cuckoo framework 做成【分散式系統】以減少惡意軟體分析時間
系統功能	使用者於網頁上提交 malware sample，在後端(分散式系統)進行樣本分析，產出 sample report
使用技術	Java Socket、Cuckoo Sandbox
系統截圖	<p style="text-align: center;">Distributed System of Cuckoo Sandbox</p> <p style="text-align: center;">Figure 15 分散式 Cuckoo 系統架構圖</p>

碩論題目:Enabling VMI-based Memory Inspection for Runtime Protection in KVM

目標	在 QEMU+KVM 中實作虛擬機器內省側錄技術(VMI)，實現對 VM 內的應用程式式呼叫的 Windows API Profiling
系統功能	在 QEMU 上使用者指定 VM 內 process name，側錄該 process 呼叫到 Windows APIs 的參數值與回傳值，並將其紀錄成檔案，以供後續分析之用
使用技術	C、QEMU+KVM、Windows API hooking、x64 Assembly
系統截圖	<p style="text-align: center;">System Architecture</p> <p style="text-align: center;">Figure 16 論文系統架構圖</p>